Peeking into the Web PKI

Uncovering the Trust That Sustains Web Server Authentication

Zane Ma (he/him)
Oregon State University
2024.05.02

Web Server Authentication

Billions of users

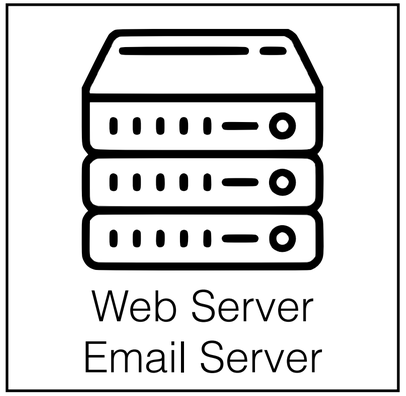
HTTPS/TLS

Millions of servers

First step in securing the Web:
messaging, websites, email, etc.

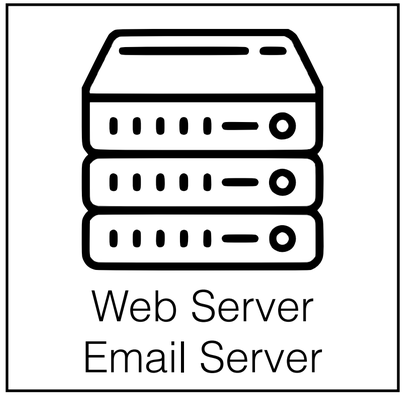
Background

paypal.com

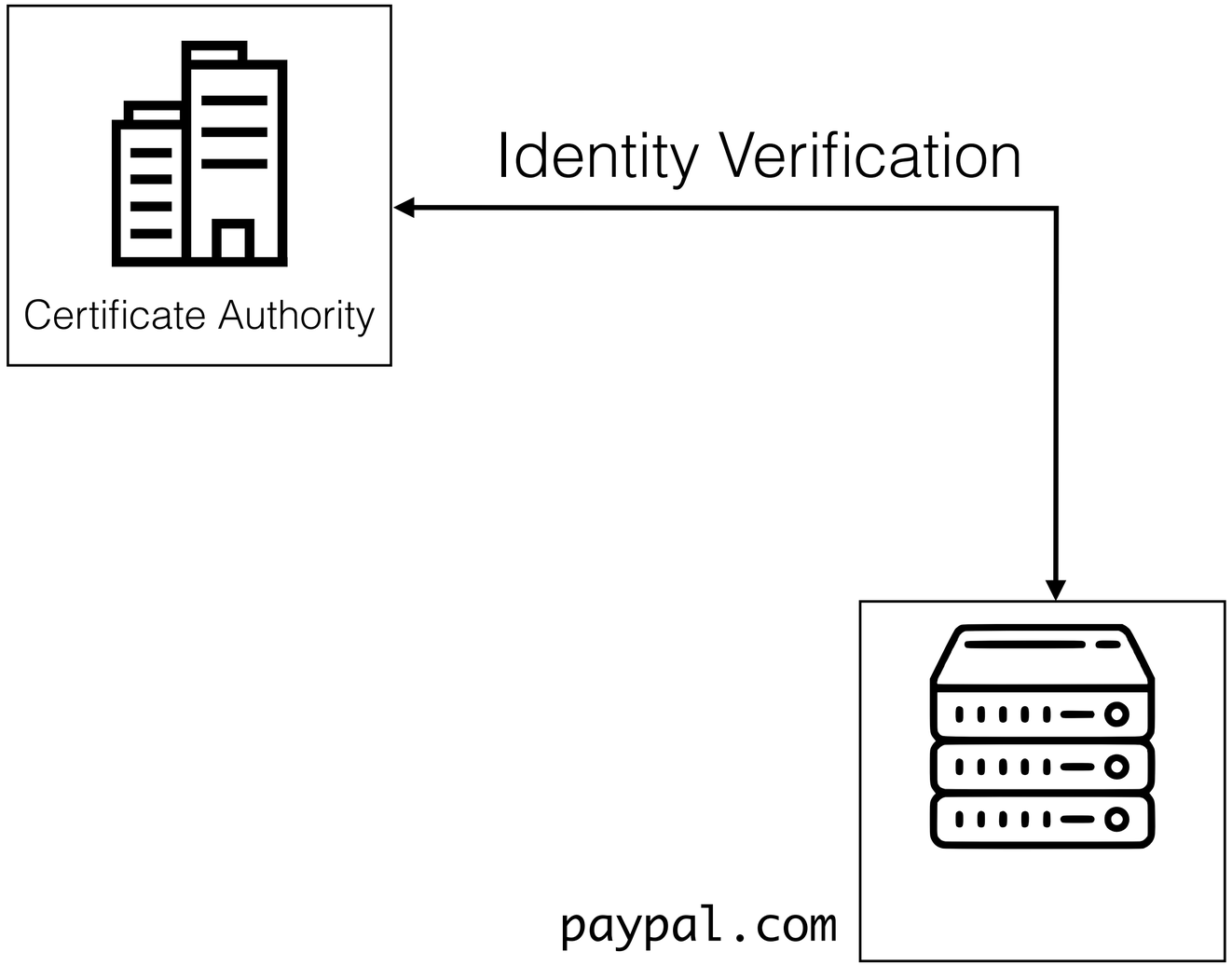


Background

paypal.com

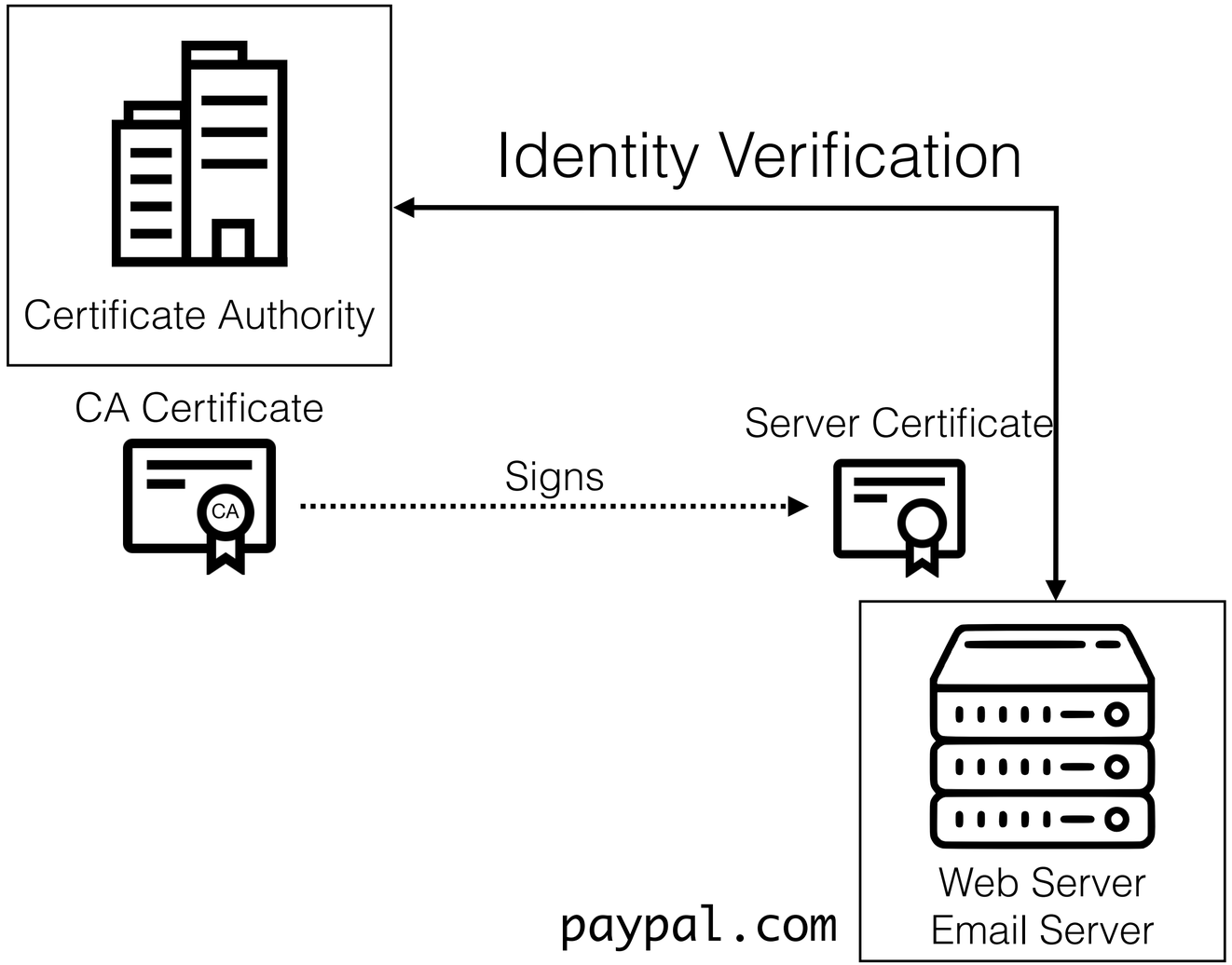


Background


Certificate Authority
Identity Verification
paypal.com

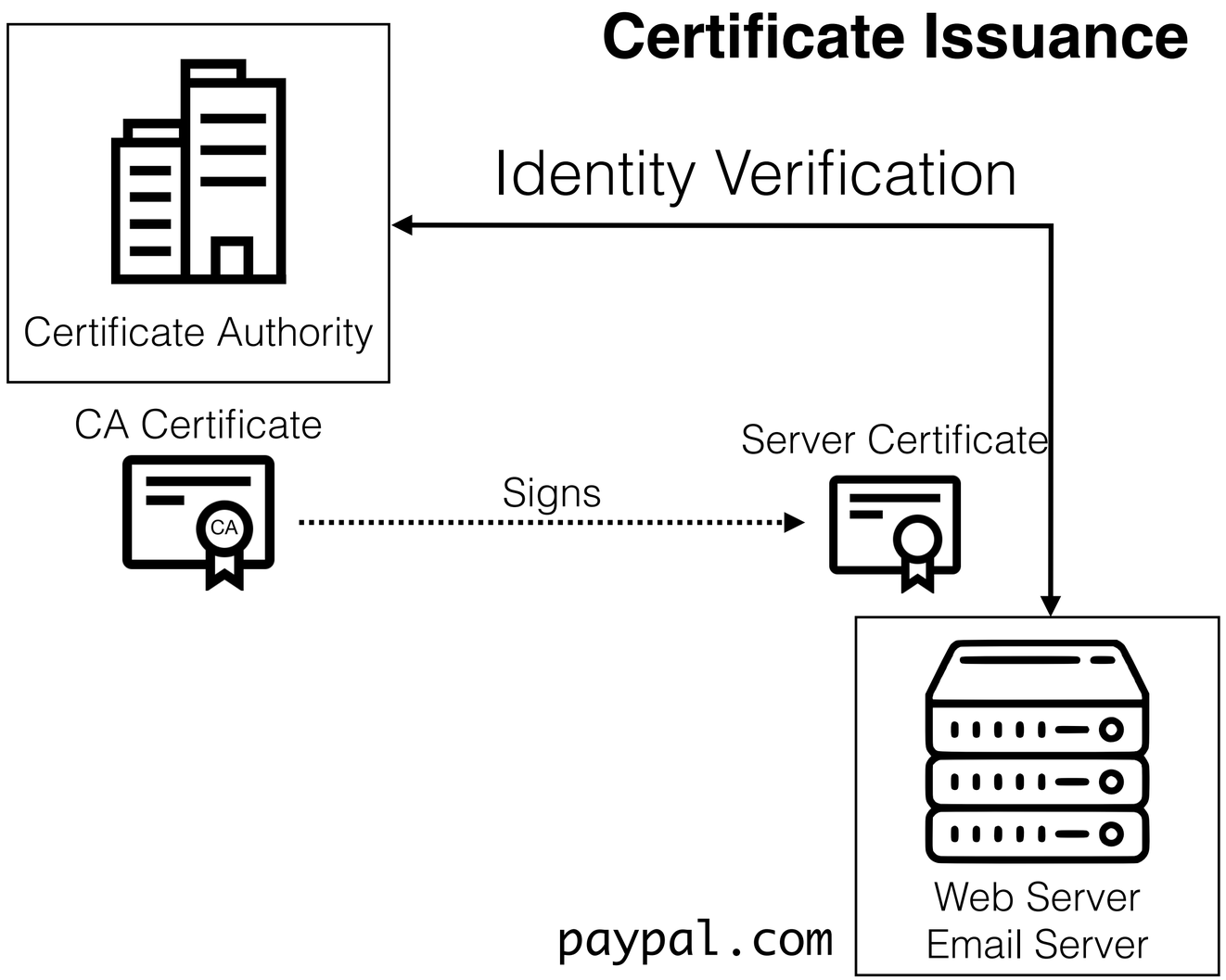
www

Background


Certificate Authority
Identity Verification
CA Certificate
CA
Signs
Server Certificate
paypal.com
Web Server
Email Server

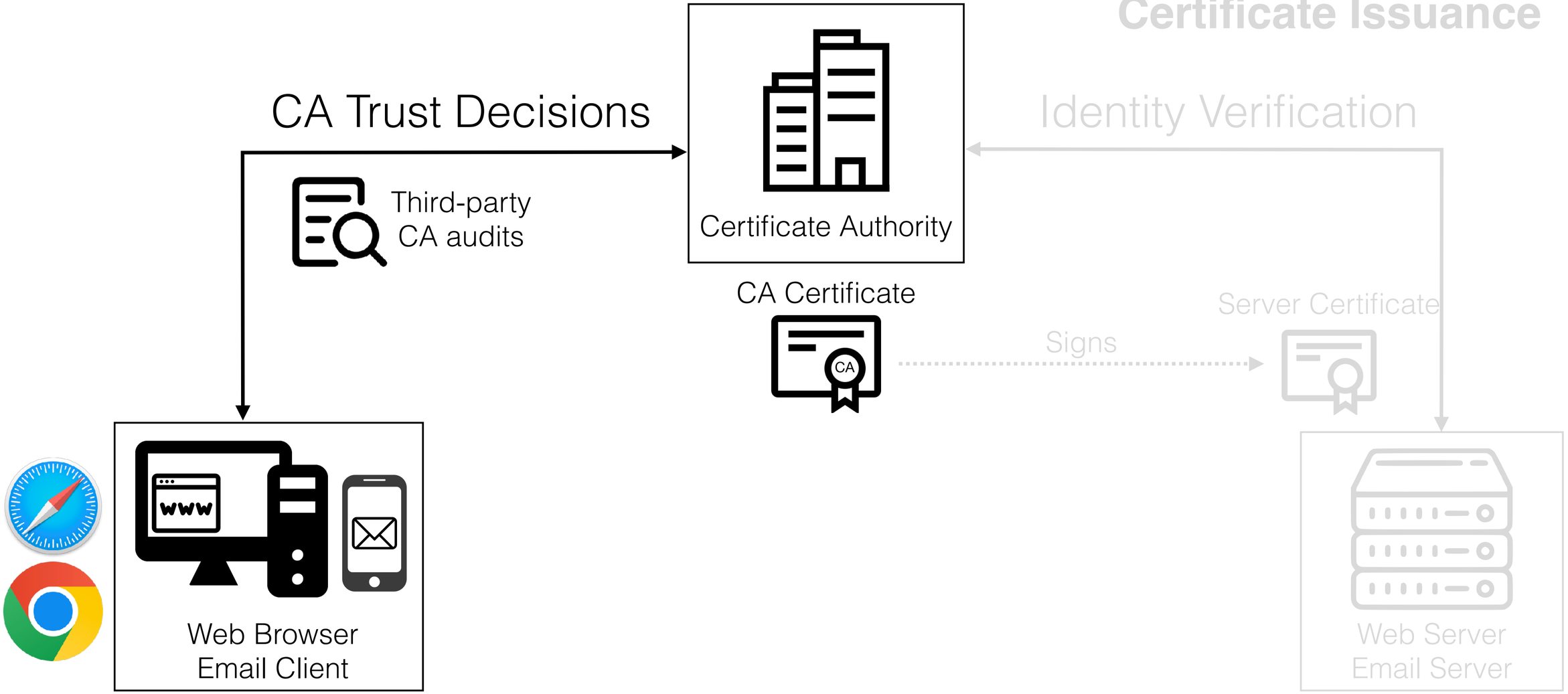
Web Browser
Email Client

Background

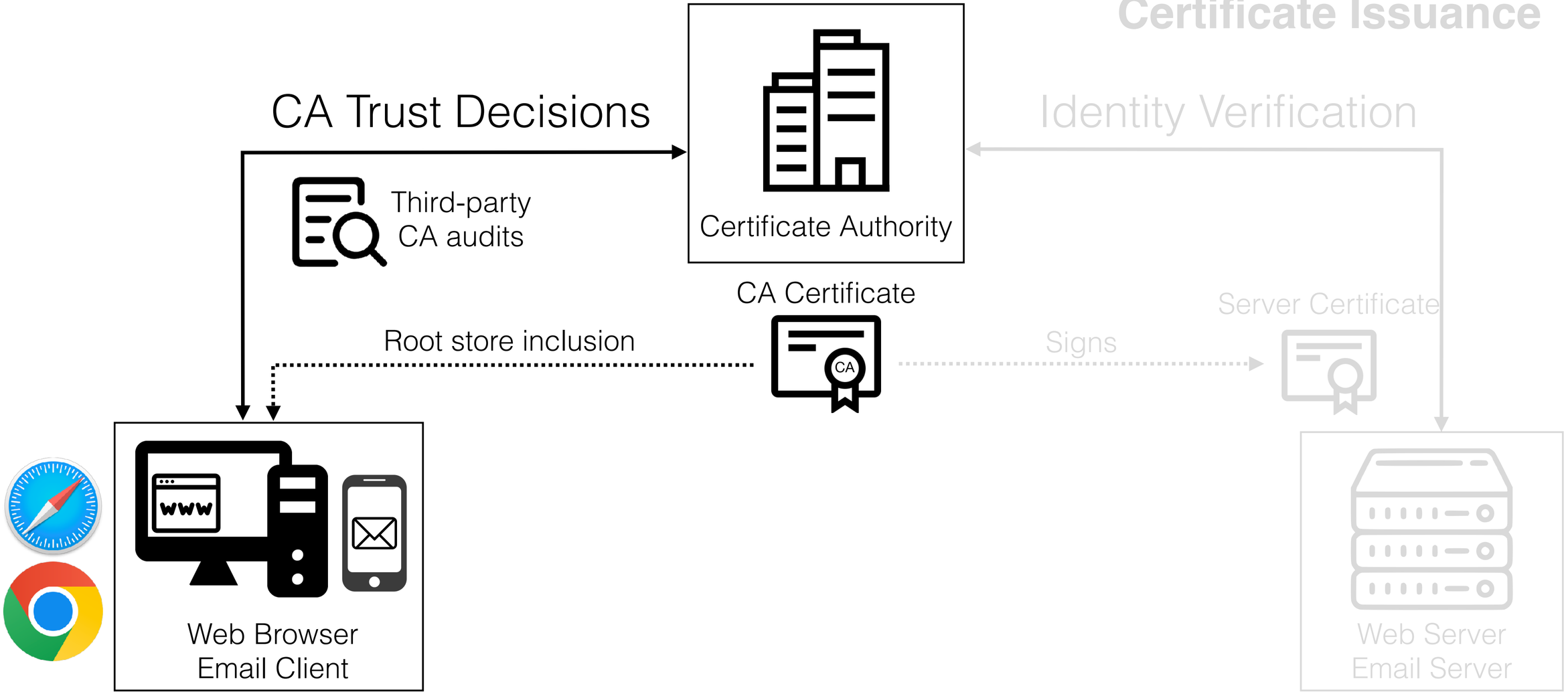

Certificate Issuance
Identity Verification
Certificate Authority
CA Certificate
CA
Signs
Server Certificate
paypal.com
Web Server
Email Server

Web Browser
Email Client

Background

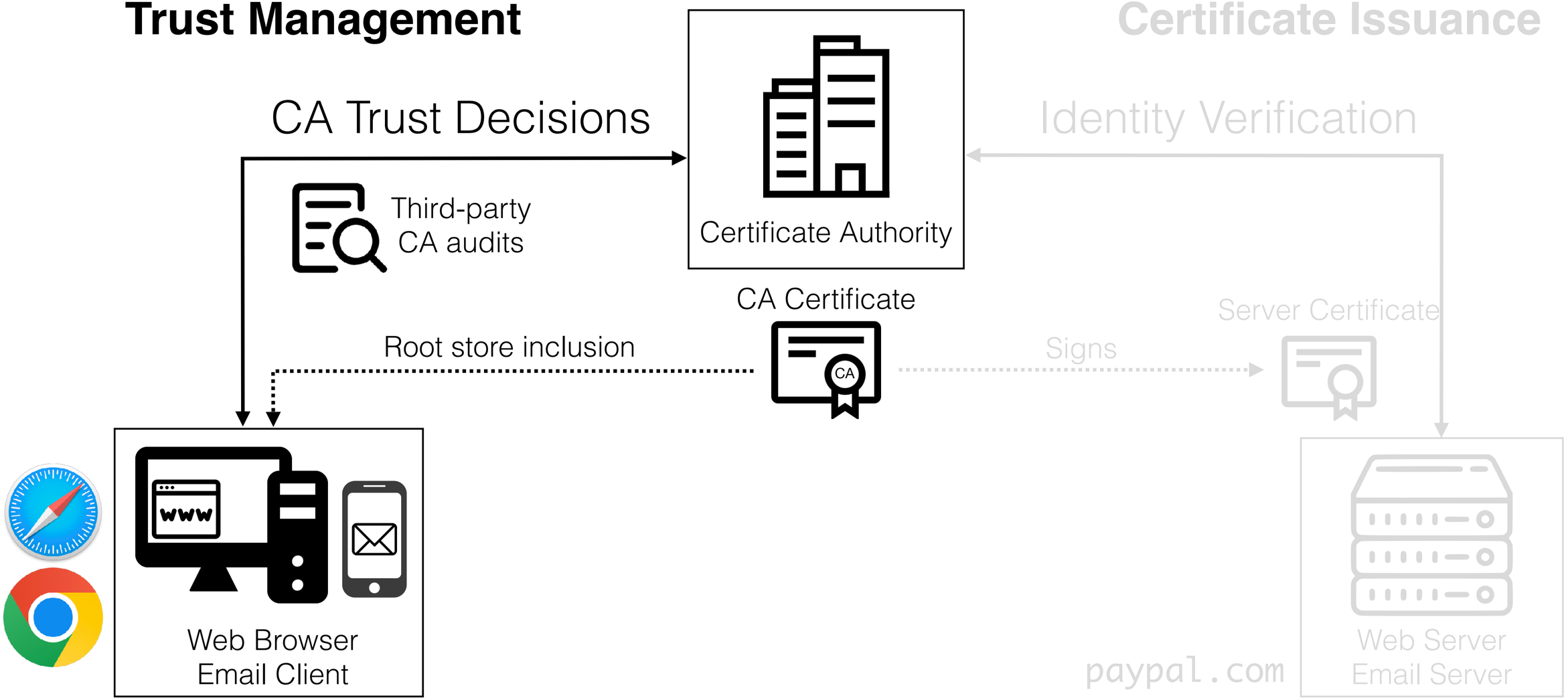

Certificate Issuance
CA Trust Decisions
Identity Verification
Third-party
CA audits
Certificate Authority
CA Certificate
CA
Server Certificate
Signs
Web Browser
Email Client
Web Server
Email Server

Background

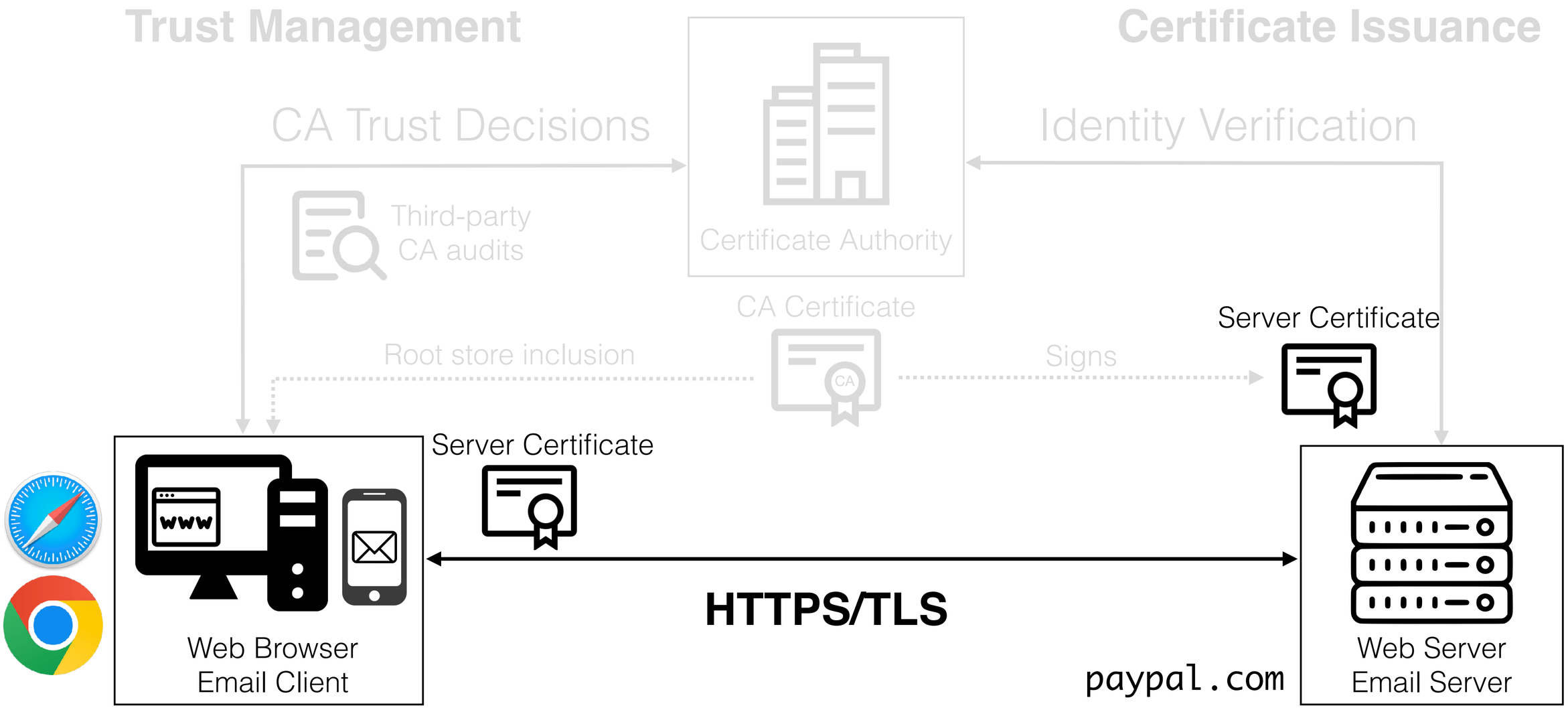

Certificate Issuance
CA Trust Decisions
Identity Verification
Third-party
CA audits
Certificate Authority
CA Certificate
Server Certificate
Root store inclusion
Signs
CA
Web Browser
Email Client
Web Server
Email Server

Background

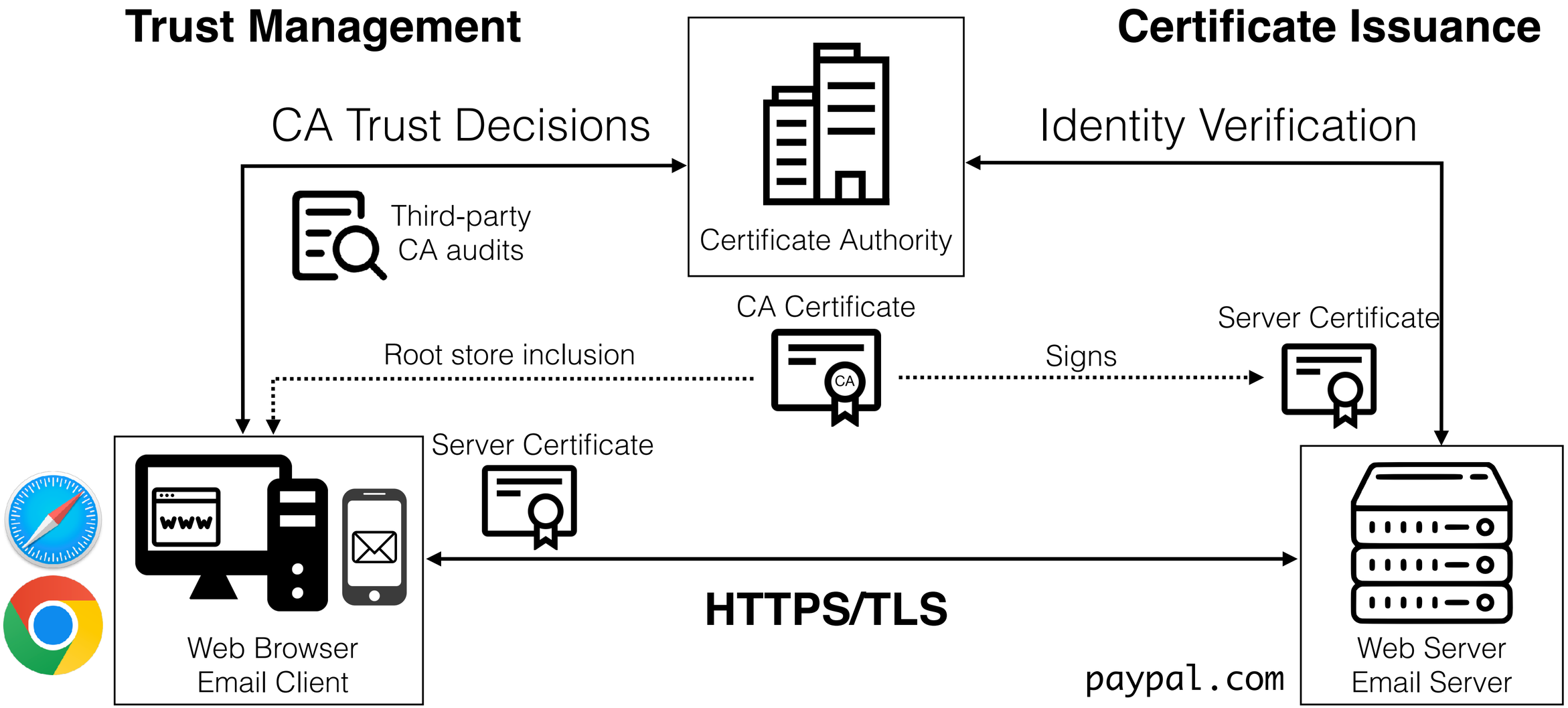
Trust Management



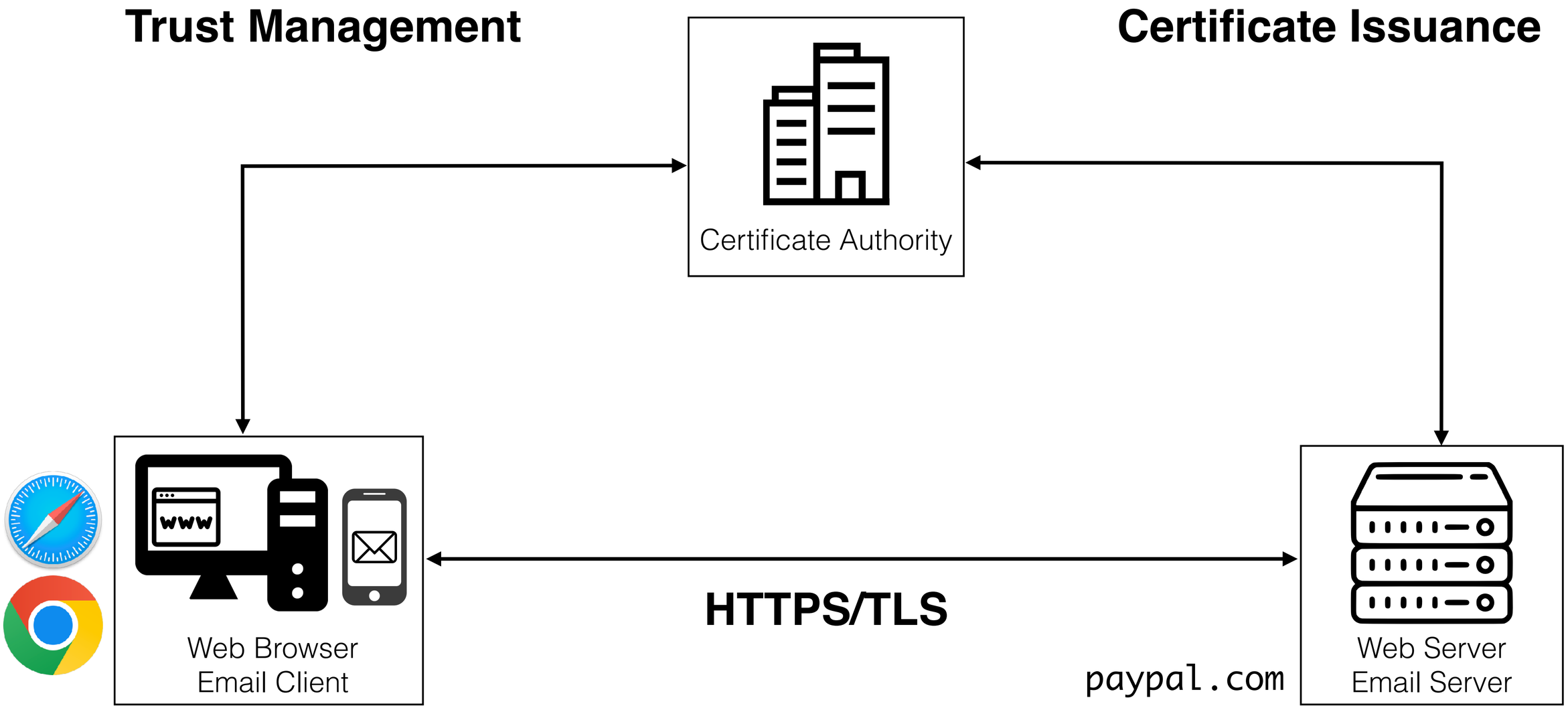
Background


Trust Management
Certificate Issuance
CA Trust Decisions
Identity Verification
Third-party
CA audits
Certificate Authority
CA Certificate
Server Certificate
Root store inclusion
Signs
CA
Server Certificate
www
Web Browser
Email Client
HTTPS/TLS
paypal.com
Web Server
Email Server

Background

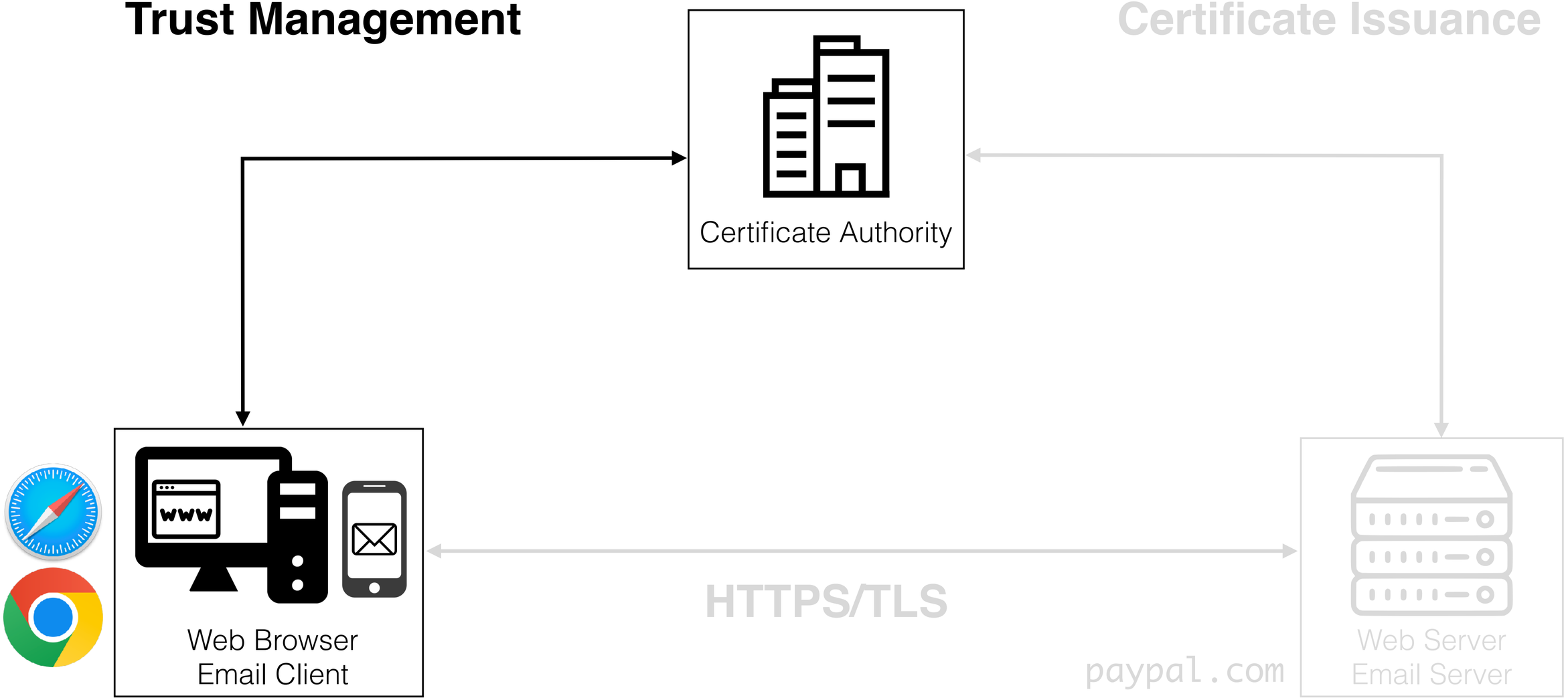

Trust Management
Certificate Issuance
CA Trust Decisions
Identity Verification
Third-party
CA audits
Certificate Authority
CA Certificate
Server Certificate
Root store inclusion
Signs
CA
Server Certificate
www
Web Browser
Email Client
HTTPS/TLS
paypal.com
Web Server
Email Server

Threat Model



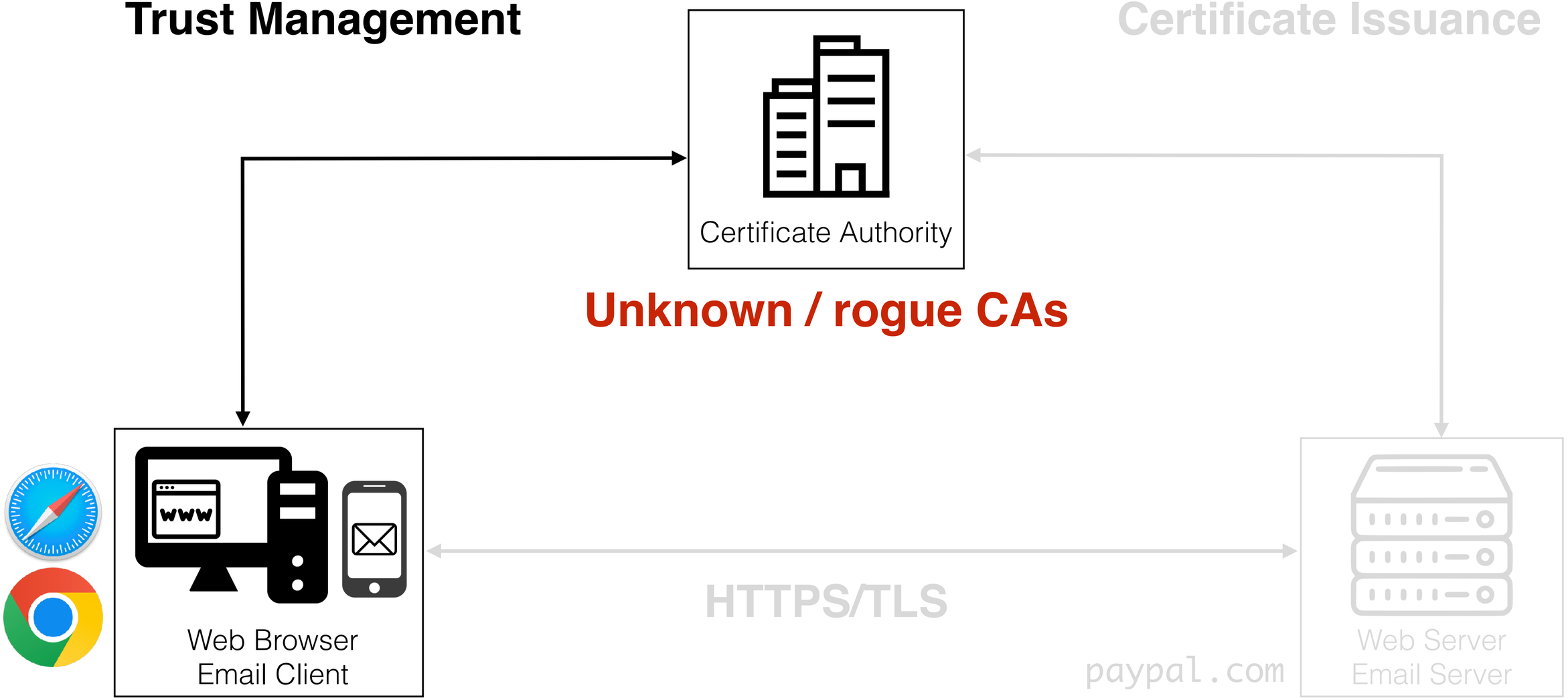
Threat Model

Trust Management



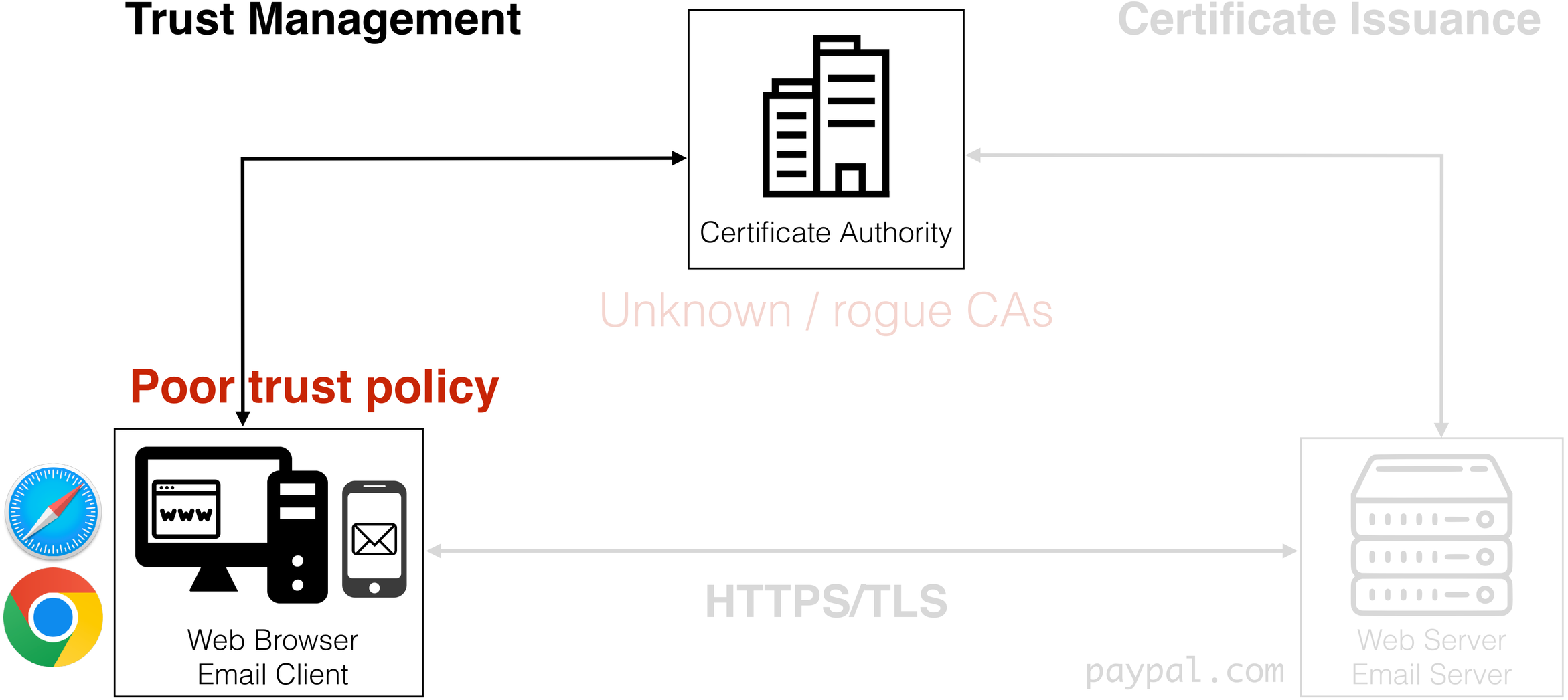
Threat Model

Trust Management



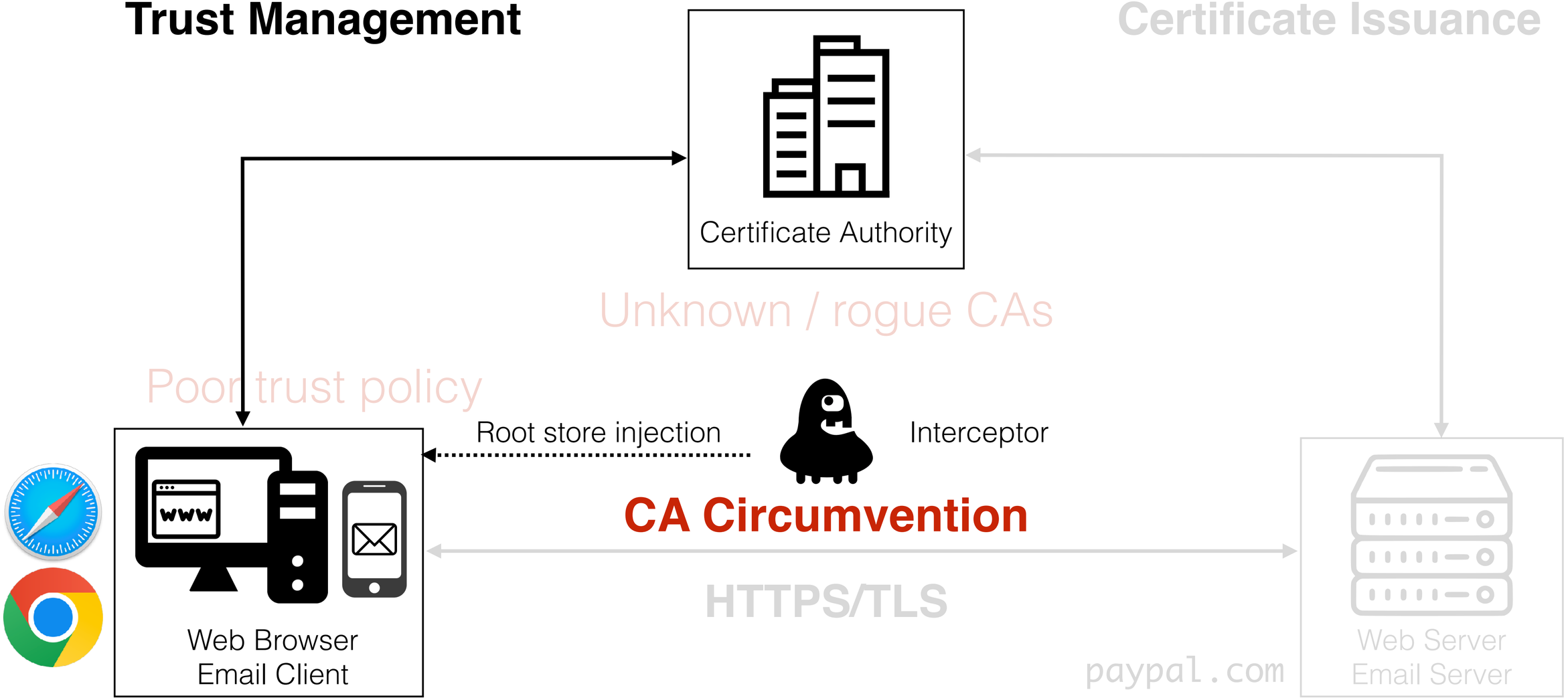
Threat Model

Trust Management

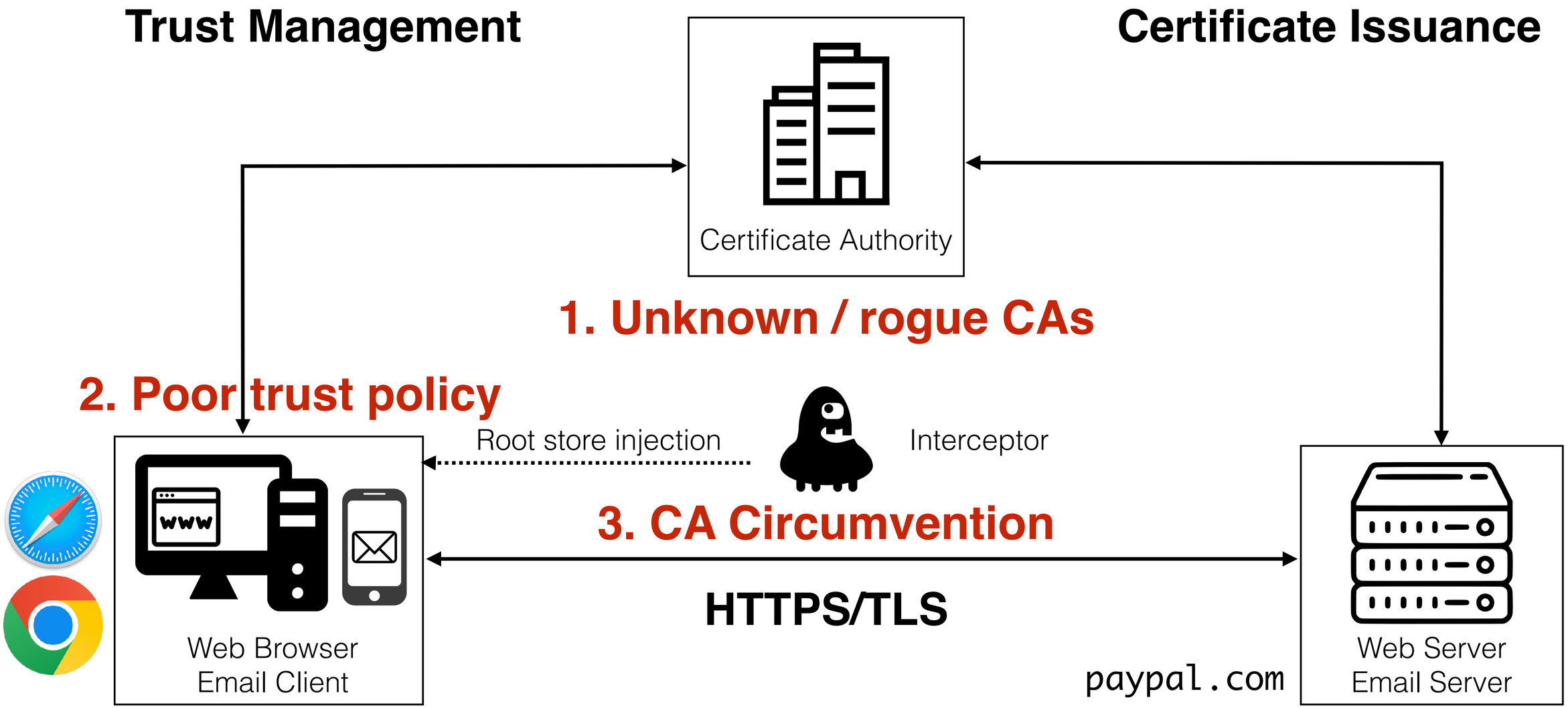


Threat Model

Trust Management



Roadmap


Trust Management
Certificate Issuance
Certificate Authority
1. Unknown / rogue CAs
2. Poor trust policy
Root store injection
Interceptor
3. CA Circumvention
HTTPS/TLS
Web Browser
Email Client
paypal.com
Web Server
Email Server

Symantec Distrust

- From 2009-2017 Symantec was responsible for over a dozen issues[1] that prompted removal from browser root stores
- Difficult to determine which CA certificates Symantec operated!

[1] https://wiki.mozilla.org/CA:Symantec_Issues

Symantec Distrust

- From 2009-2017 Symantec was responsible for over a dozen issues[1] that prompted removal from browser root stores

- Difficult to determine which CA certificates Symantec operated!

```
commonName           = UTN-USERFirst-Client Authentication and Email
orgUnitName          = http://www.usertrust.com
orgName              = The USERTRUST Network
localityName         = Salt Lake City
stateOrProvinceName  = UT
countryName          = US
```

CA cert #1

```
commonName           = UTN-USERFirst-NetworkApplications
orgUnitName          = http://www.usertrust.com
orgName              = The USERTRUST Network
localityName         = Salt Lake City
stateOrProvinceName  = UT
countryName          = US
```

CA cert #2

[1] https://wiki.mozilla.org/CA:Symantec_Issues

Symantec Distrust

- From 2009-2017 Symantec was responsible for over a dozen issues[1] that prompted removal from browser root stores

- Difficult to determine which CA certificates Symantec operated!

```
commonName          = UTN-USERFirst-Client Authentication and Email
orgUnitName         = http://www.usertrust.com
orgName             = The USERTRUST Network
localityName        = Salt Lake City
stateOrProvinceName = UT
countryName         = US
```

Comodo CA cert #1

```
commonName          = UTN-USERFirst-NetworkApplications
orgUnitName         = http://www.usertrust.com
orgName             = The USERTRUST Network
localityName        = Salt Lake City
stateOrProvinceName = UT
countryName         = US
```

Symantec CA cert #2

[1] https://wiki.mozilla.org/CA:Symantec_Issues

Observations

1. Gap between what is trusted (CAs) and how it is enforced (CA certificates).

Observations

1. Gap between what is trusted (CAs) and how it is enforced (CA certificates).

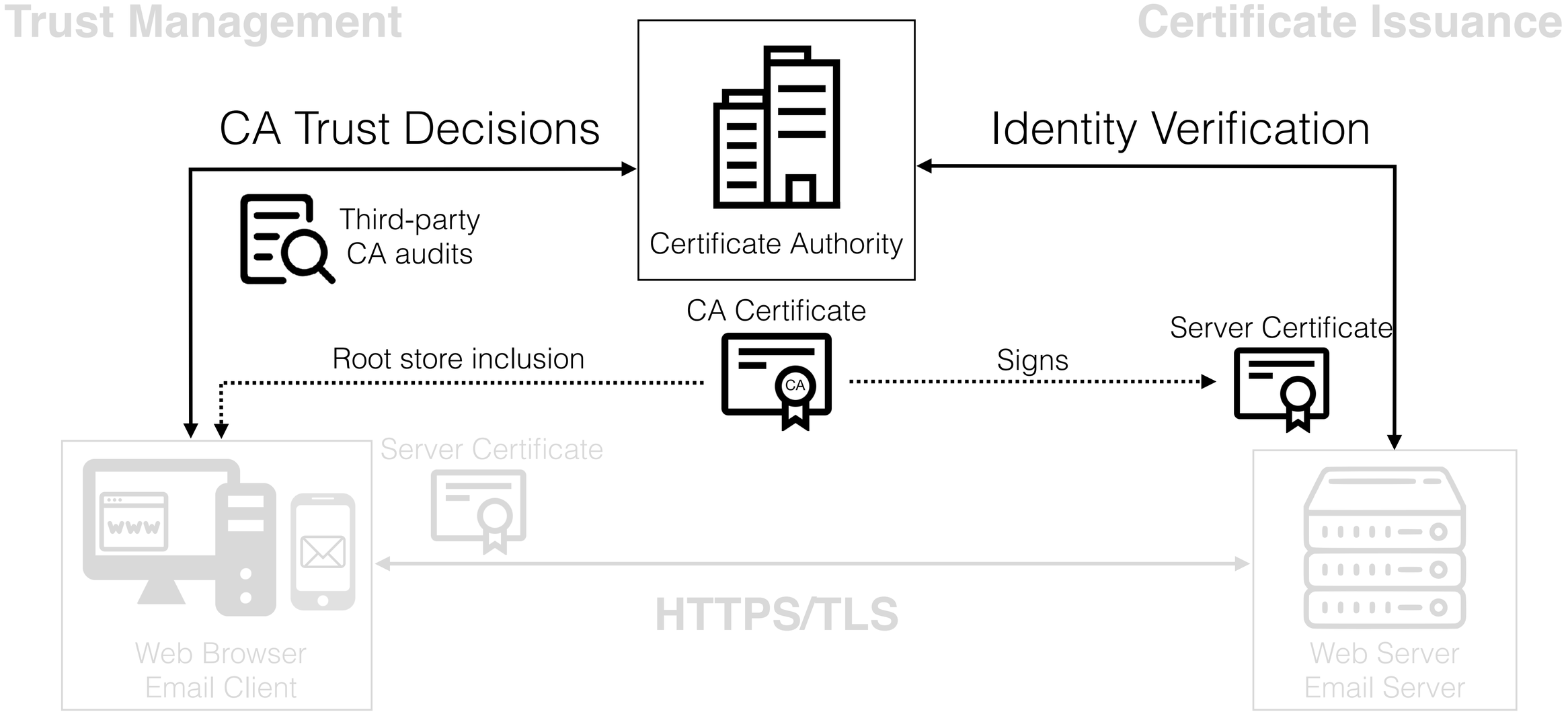
2. There are no guarantees that the identity in a CA certificate reflects the operator of the CA certificate.

Approach

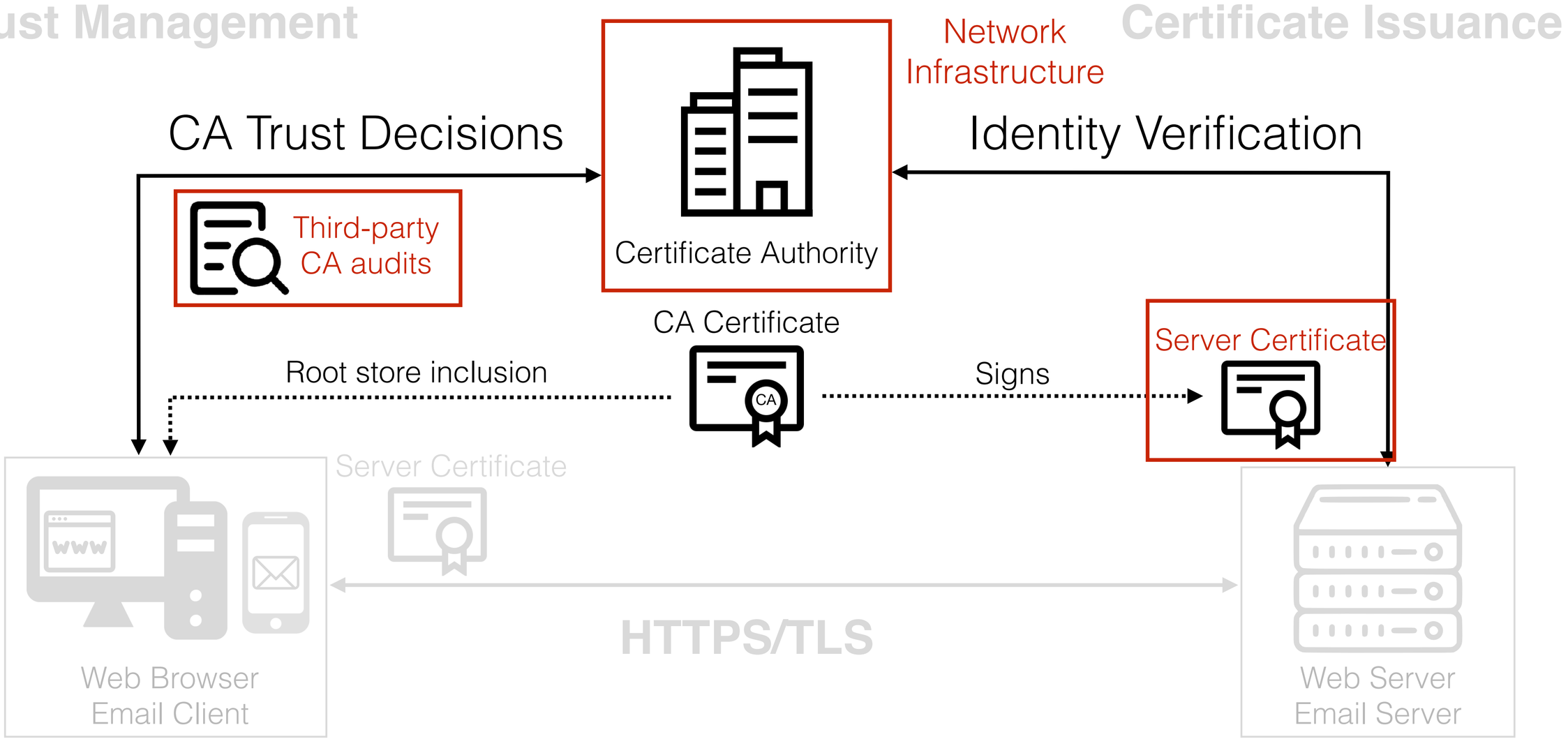
How can we build a system to determine the *operator* of a CA certificate / issuer?

1. Measure CA operational features

Perspectives on CA Operations



Perspectives on CA Operations



Approach

1. Measure CA operational features

Audits

+

Network Infra.

+

Certificates

Approach

1. Measure CA operational features

+

+

Audits

Reports from in-person visits to CA facilities

Incomplete; only verify minimum requirements or what is self-reported

Network Infra.

Certificates

Approach

1. Measure CA operational features

+

+

Audits	Network Infra.	Certificates
Reports from in-person visits to CA facilities	Direct measurement of CA functional endpoint	
Incomplete; only verify minimum requirements or what is self-reported	Often obscured by network indirection (e.g., CDNs)	

Approach

1. Measure CA operational features

+

+

Audits	Network Infra.	Certificates
Reports from in-person visits to CA facilities	Direct measurement of CA functional endpoint	Goal: distinctive measurement of a CA's certificate issuance process
Incomplete; only verify minimum requirements or what is self-reported	Often obscured by network indirection (e.g., CDNs)	

Certificate Fingerprints

Certificate Fingerprints

```
Certificate root
   TBS certificate
      Validity
         datetime:start
         datetime:end
      Subject
         Field
            oid:commonName
            string:name
         Field
            oid:organizationName
            string:name
      Extensions
         Extension
            oid:keyUsage
         Extension
            oid:basicConstraints
   Signature
      oid:sha256WithRSAEnc.
      bytes:signatureValue
```

Certificate Fingerprints

```
Certificate root
   TBS certificate
      Validity
         datetime:start
         datetime:end
      Subject
         Field
            oid:commonName
            string:name
         Field
            oid:organizationName
            string:name
      Extensions
         Extension
            oid:keyUsage
         Extension
            oid:basicConstraints
   Signature
      oid:sha256WithRSAEnc.
      bytes:signatureValue
```

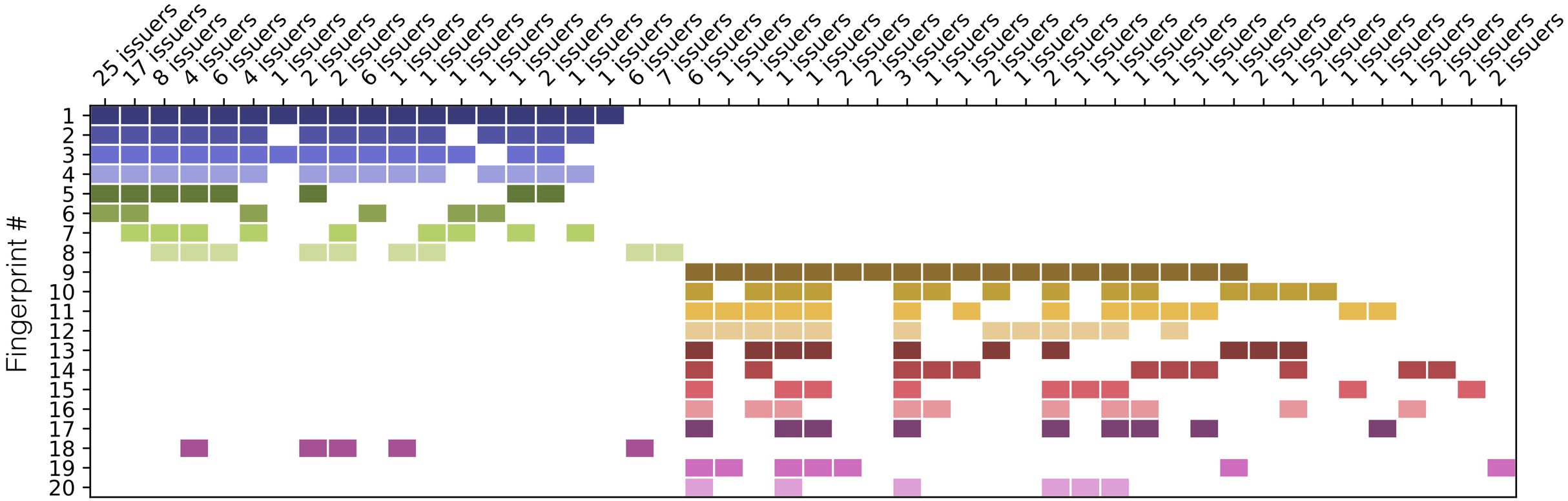
Certificate Fingerprints

```
Certificate root
   TBS certificate
      Validity
         datetime:start
         datetime:end
      Subject
         Field
            oid:commonName
            string:name
         Field
            oid:organizationName
            string:name
      Extensions
         Extension
            oid:keyUsage
         Extension
            oid:basicConstraints
   Signature
      oid:sha256WithRSAEnc.
      bytes:signatureValue
```

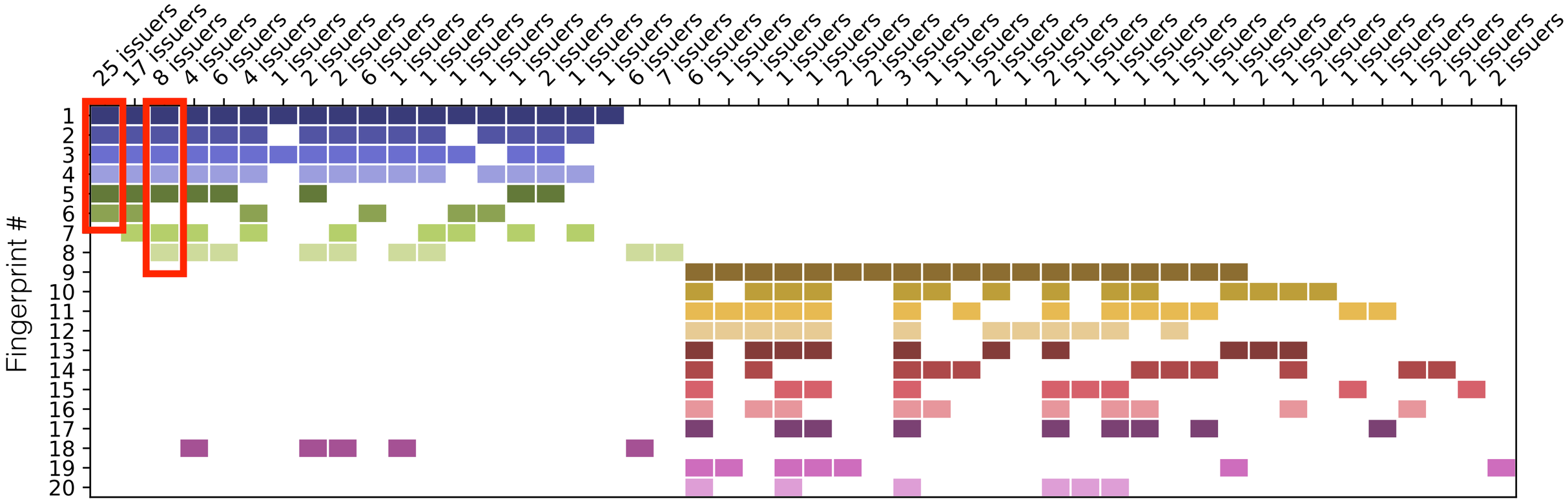
Certificate Fingerprints

```
Certificate root
   TBS certificate
      Validity
         datetime:
         datetime:
      Subject
         Field
            oid:commonName
            string:
         Field
            oid:organizationName
            string:
      Extensions
         Extension
            oid:keyUsage
         Extension
            oid:basicConstraints
   Signature
      oid:sha256WithRSAEnc.
      bytes:
```

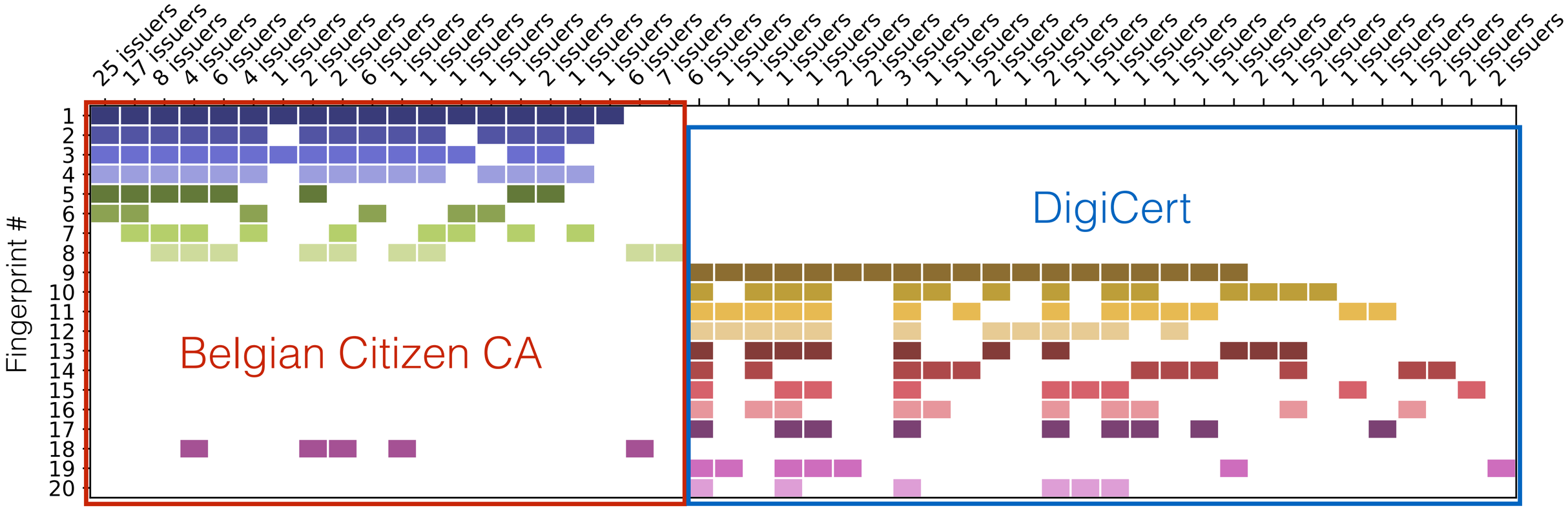
Certificate Fingerprints



Certificate Fingerprints



Certificate Fingerprints



Approach

1. Measure CA operational features

Audits

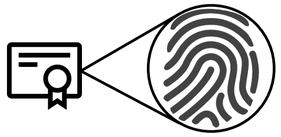
Reports from in-person visits to CA facilities

Incomplete; only verify minimum requirements or what is self-reported

Network Infra.

Direct measurement of CA functional endpoint

Often obscured by network indirection (e.g., CDNs)



Cert. Fingerprints

Isolates core CA operation - certificate issuance software

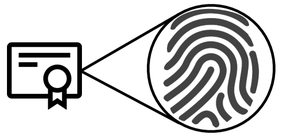
High precision, retroactive detection

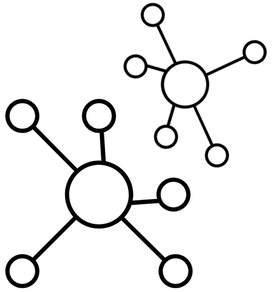
Approach

1. Measure CA operational features

+

+





CA operator clusters

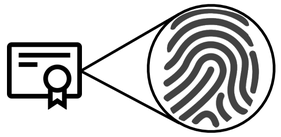
Audits	Network Infra.	Cert. Fingerprints
Reports from in-person visits to CA facilities	Direct measurement of CA functional endpoint	Isolates core CA operation - certificate issuance software
Incomplete; only verify minimum requirements or what is self-reported	Often obscured by network indirection (e.g., CDNs)	High precision, retroactive detection

Approach

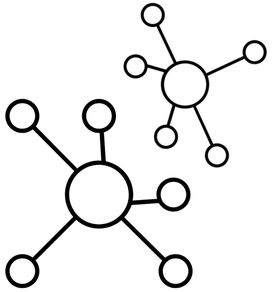
1. Measure CA operational features

+

+



Audits	Network Infra.	Cert. Fingerprints
Reports from in-person visits to CA facilities	Direct measurement of CA functional endpoint	Isolates core CA operation - certificate issuance software
Incomplete; only verify minimum requirements or what is self-reported	Often obscured by network indirection (e.g., CDNs)	High precision, retroactive detection



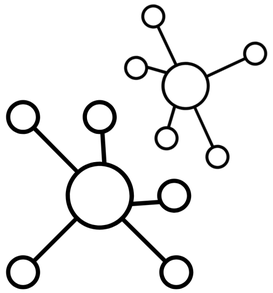
CA operator clusters

Unlabeled!

Approach

How can we build a system to determine the *operator* of a CA certificate / issuer?

1. Measure CA operational features

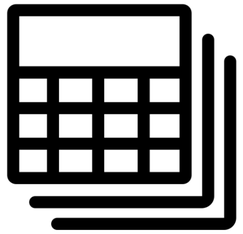


CA operator clusters

+

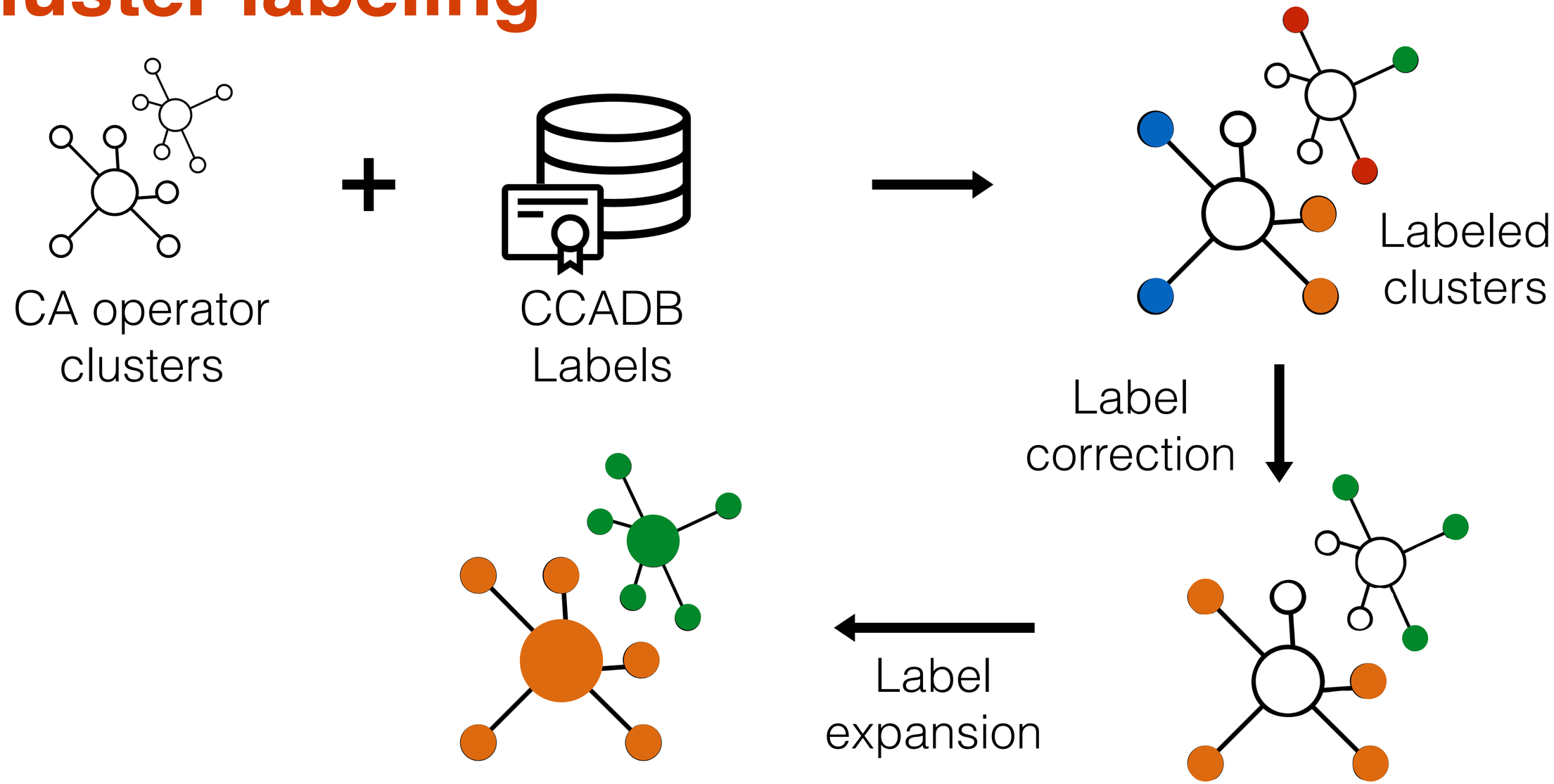
CCADB Labels

Label correction and expansion →

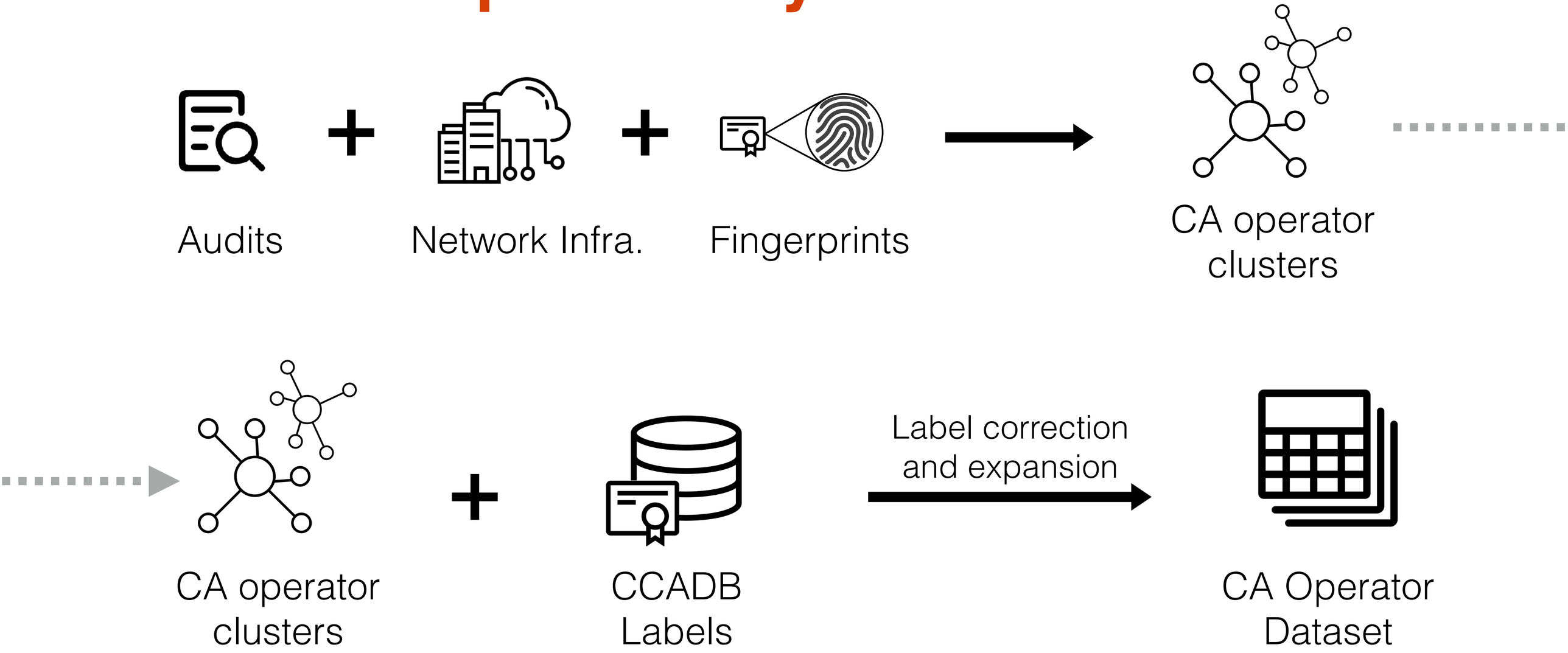


CA Operator Dataset

Cluster labeling



Fides: CA Operator System



Results

Finding	Outcome
Found trusted rogue CA (MULTICERT)[1] harbored by Camerfirma CA	Camerfirma removed from Mozilla root store, distrusted by Google products + Apple

[1] https://bugzilla.mozilla.org/show_bug.cgi?id=1672029
[2] https://bugzilla.mozilla.org/show_bug.cgi?id=1727204
[3] https://bugzilla.mozilla.org/show_bug.cgi?id=1727205

Results

Finding	Outcome
Found trusted rogue CA (MULTICERT)[1] harbored by Camerfirma CA	Camerfirma removed from Mozilla root store, distrusted by Google products + Apple
Identified 892 (13% of all CA certificates) unknown or misidentified CA certificates	CCADB added automated CA consistency checking [2] and ownership annotation [3]

[1] https://bugzilla.mozilla.org/show_bug.cgi?id=1672029
[2] https://bugzilla.mozilla.org/show_bug.cgi?id=1727204
[3] https://bugzilla.mozilla.org/show_bug.cgi?id=1727205

Results

Finding	Outcome
Found trusted rogue CA (MULTICERT)[1] harbored by Camerfirma CA	Camerfirma removed from Mozilla root store, distrusted by Google products + Apple
Identified 892 (13% of all CA certificates) unknown or misidentified CA certificates	CCADB added automated CA consistency checking [2] and ownership annotation [3]

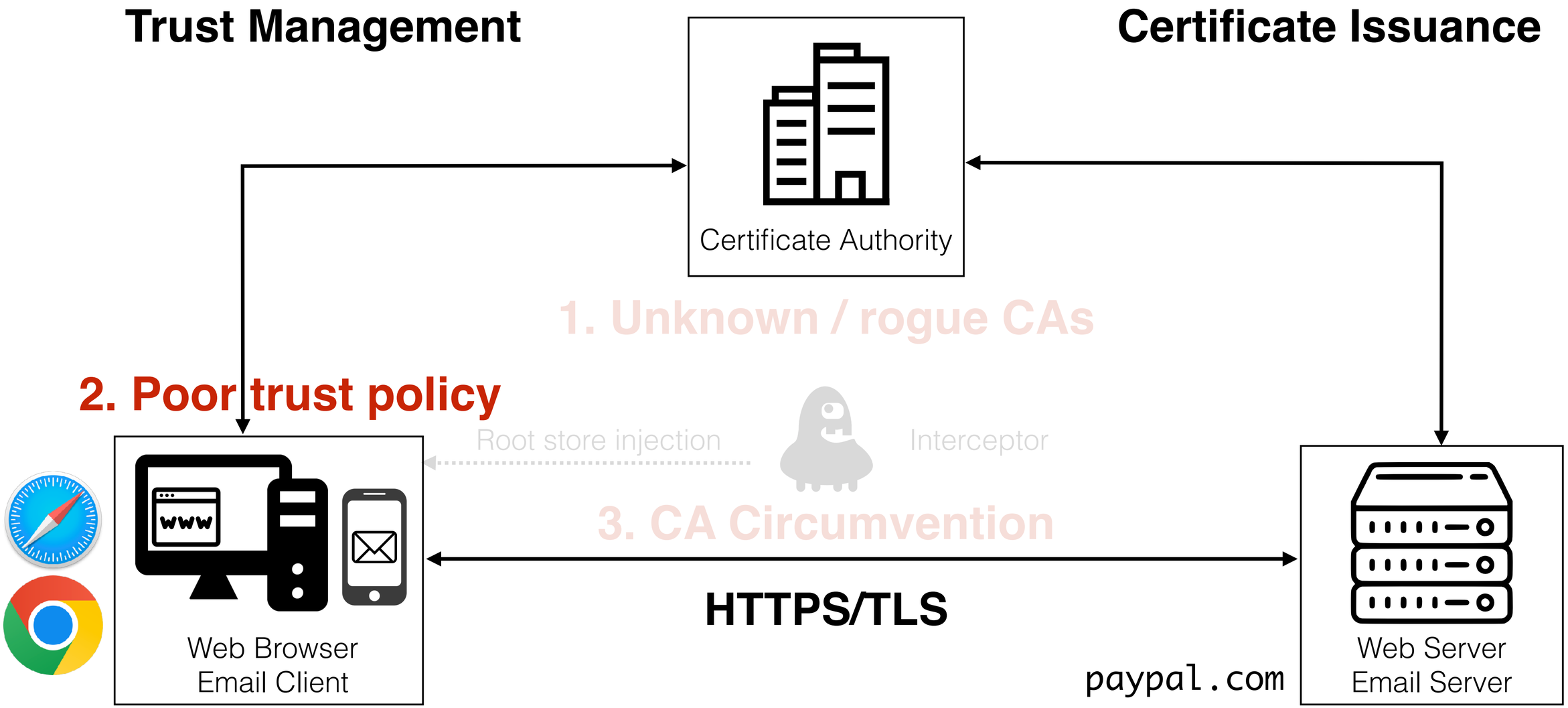
CA operational **transparency** means:

1) More accurate data for issuer attribution

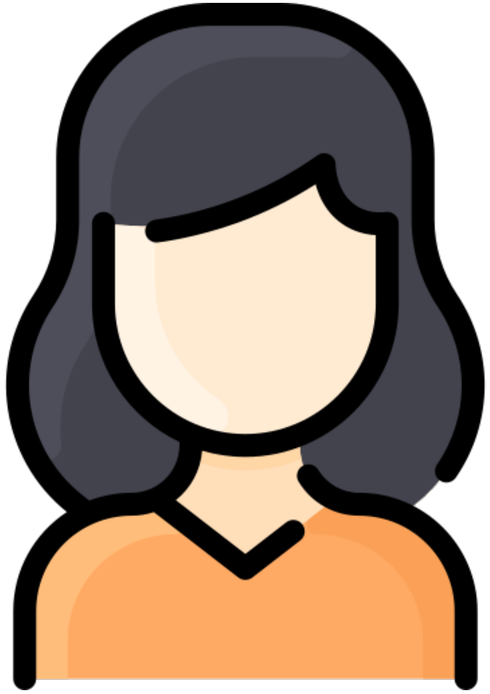
2) More informed root store decision making

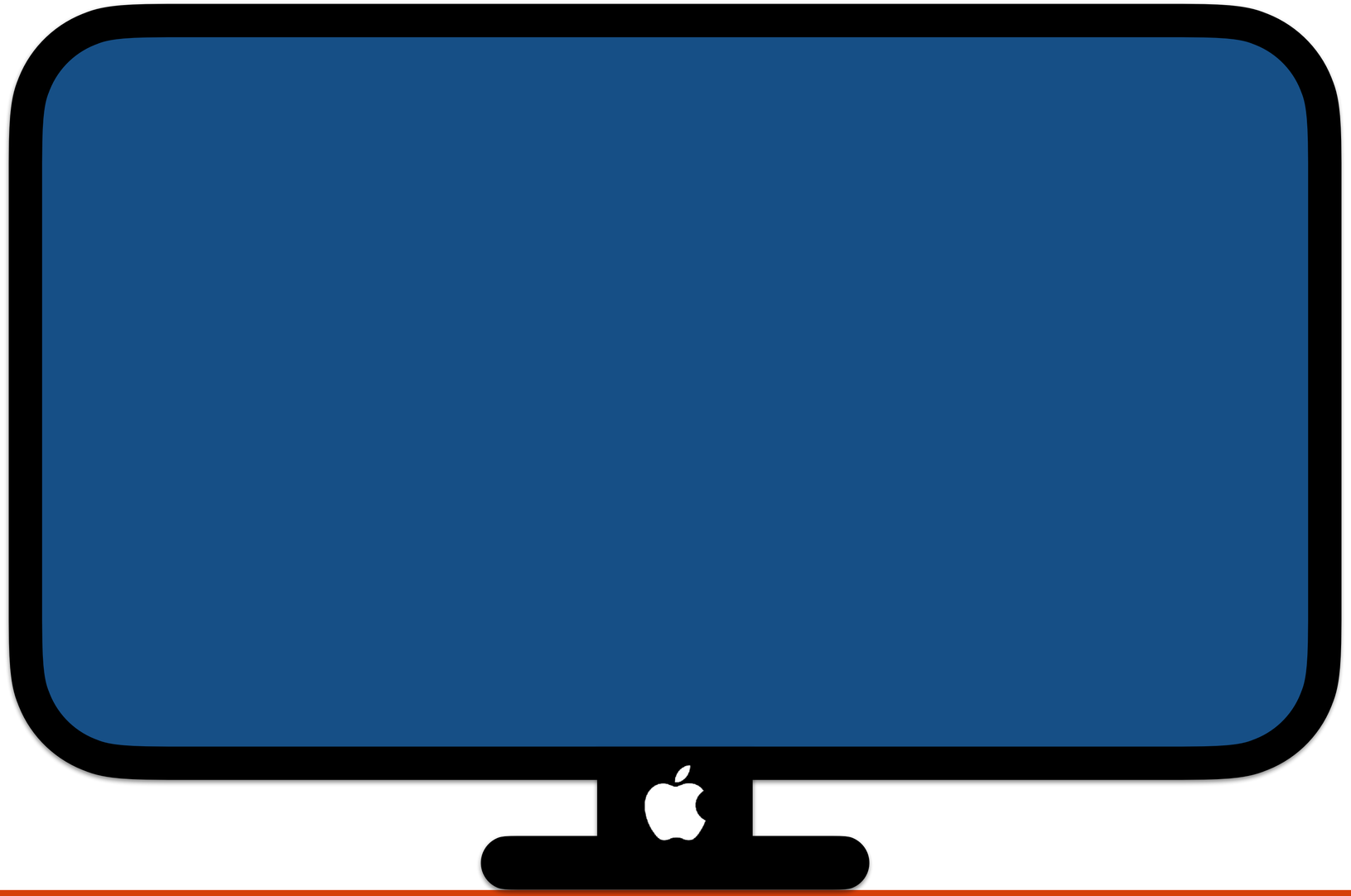
[1] https://bugzilla.mozilla.org/show_bug.cgi?id=1672029
[2] https://bugzilla.mozilla.org/show_bug.cgi?id=1727204
[3] https://bugzilla.mozilla.org/show_bug.cgi?id=1727205

Roadmap

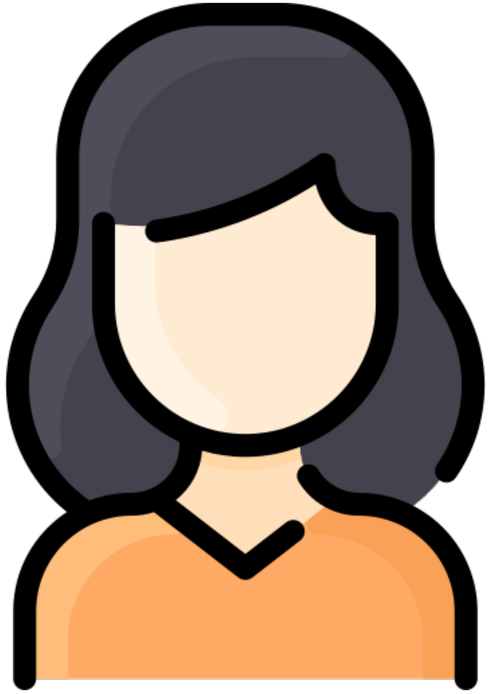

Trust Management
Certificate Issuance
Certificate Authority
1. Unknown / rogue CAs
2. Poor trust policy
Root store injection
Interceptor
3. CA Circumvention
HTTPS/TLS
Web Browser
Email Client
paypal.com
Web Server
Email Server

TLS user agents

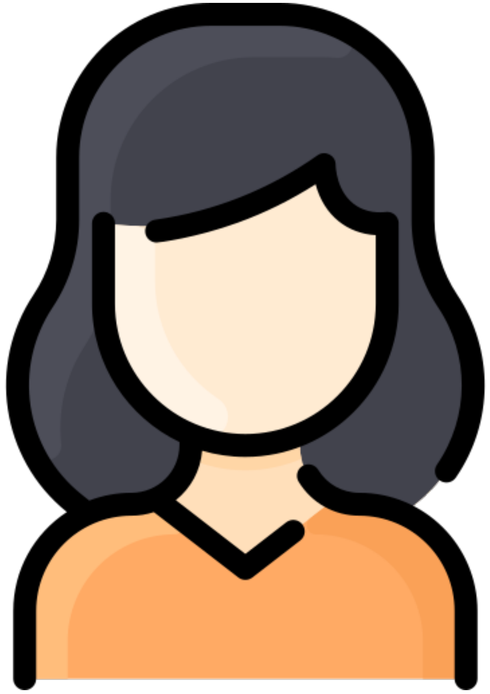




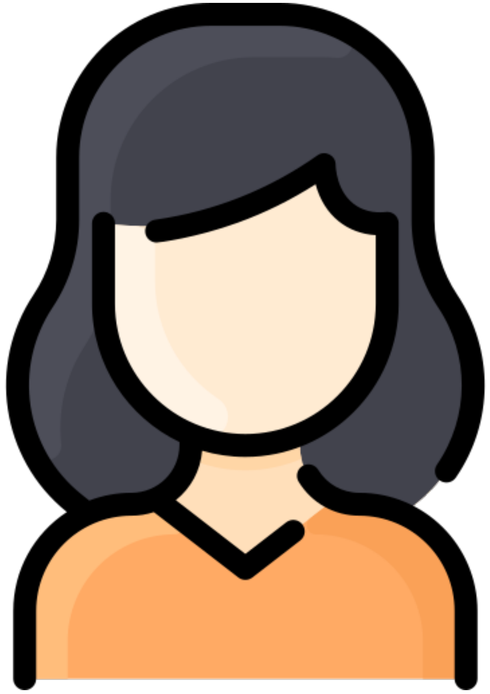
TLS user agents



TLS user agents

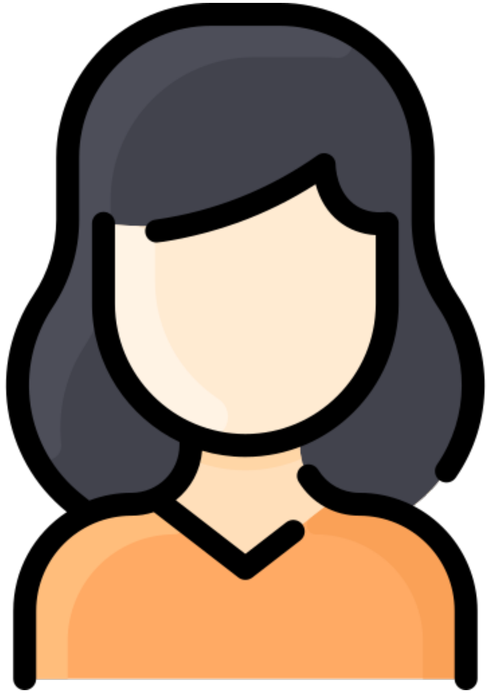


TLS user agents



TLS user agents

TLS user agents



Research Questions

1. Which root store providers do TLS user agents rely on?
2. How do root store providers determine which CAs to trust?
3. Characterization of root store programs
4. How faithfully do providers copy root program trust?

TLS user agents

Challenge: Lots of TLS user agents

TLS user agents

Challenge: Lots of TLS user agents

Approach:

1) Study popular user agents, look at the top 200 for global CDN

2) Best-effort collection of popular libraries / clients / OSes

TLS user agents

Challenge: Lots of TLS user agents

Approach:

1) Study popular user agents, look at the top 200 for global CDN

2) Best-effort collection of popular libraries / clients / OSes

Limitations: misses the long tail of TLS authentication trust

Data collection

User Agents

Web Browsers

- Chrome
- Chrome Mobile
- Opera
- Firefox
- Safari
- Mobile Safari
- Edge
- IE
- Chromium

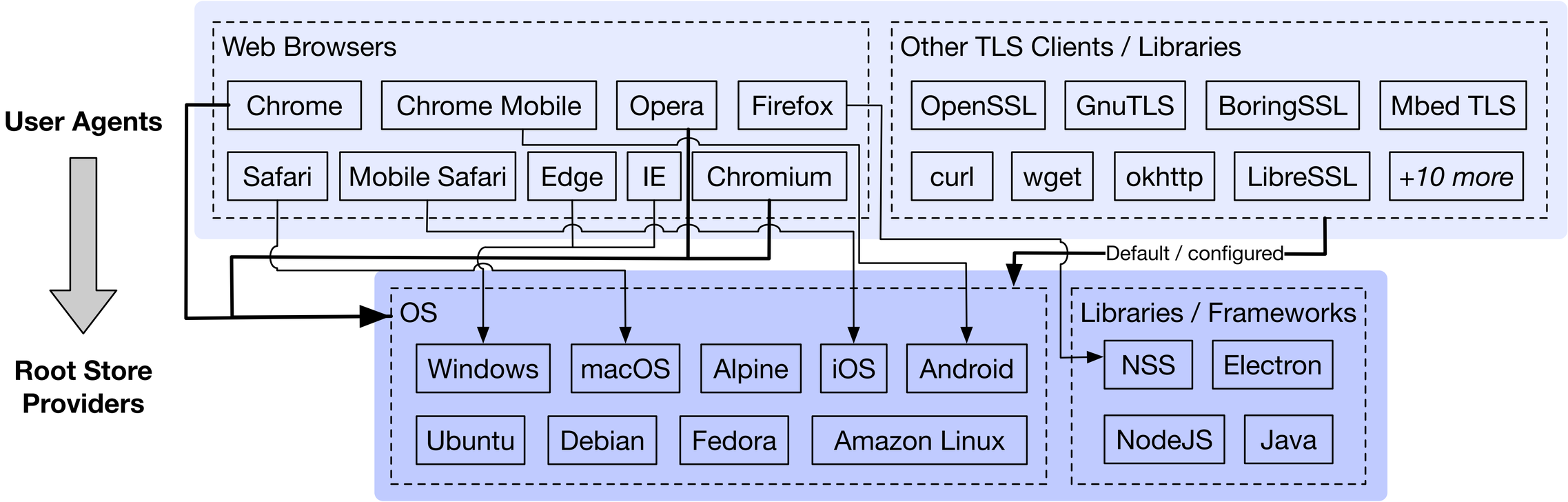
Other TLS Clients / Libraries

- OpenSSL
- GnuTLS
- BoringSSL
- Mbed TLS
- curl
- wget
- okhttp
- LibreSSL
- *+10 more*

Collected root stores for 83% of global CDN top 200 user agents

Determined default root store for dozens of libraries / TLS clients

Root store providers



Research Questions

1. Which root store providers do TLS user agents rely on?

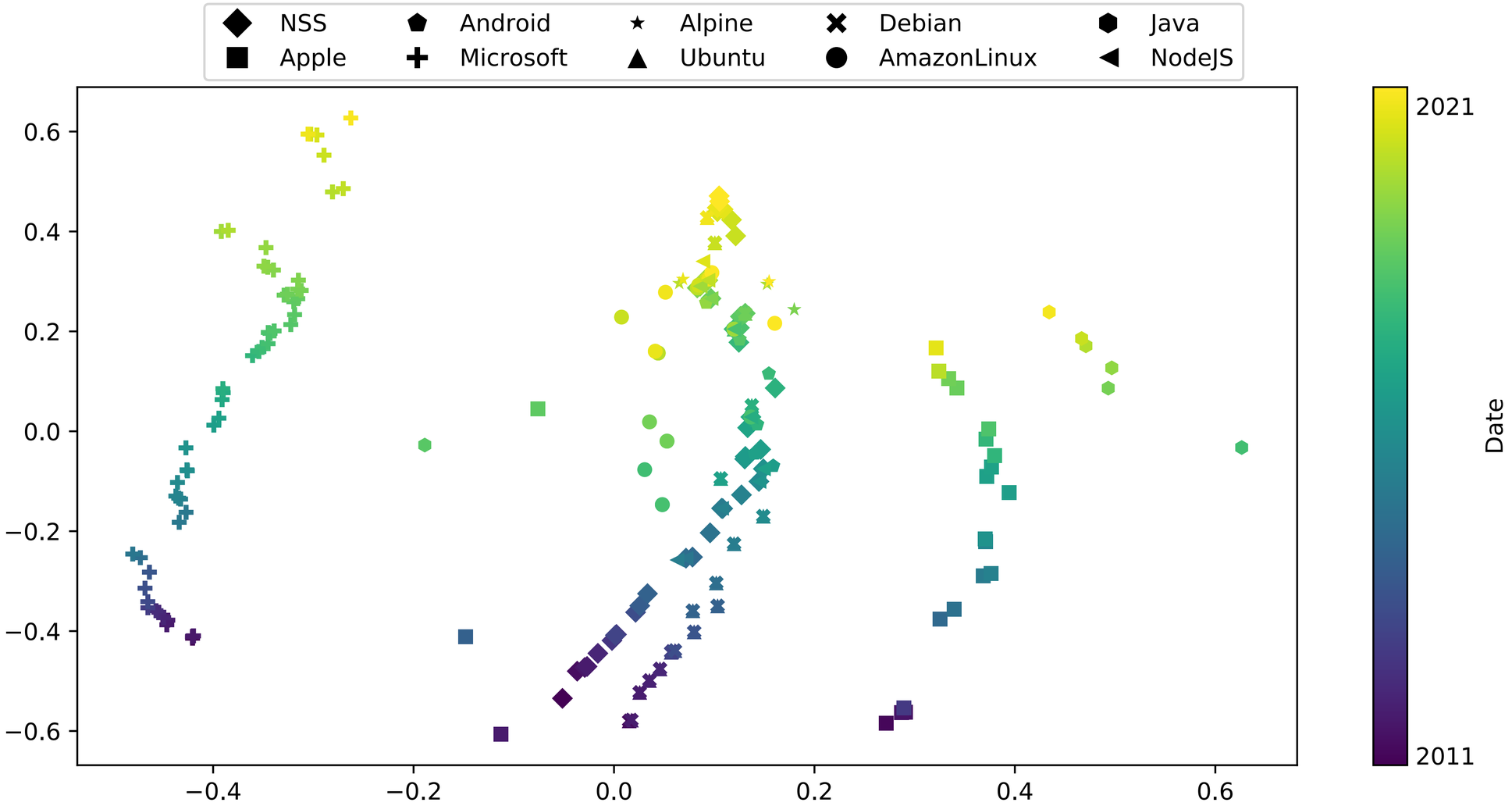
2. How do root store providers determine which CAs to trust?

3. Characterization of root store programs

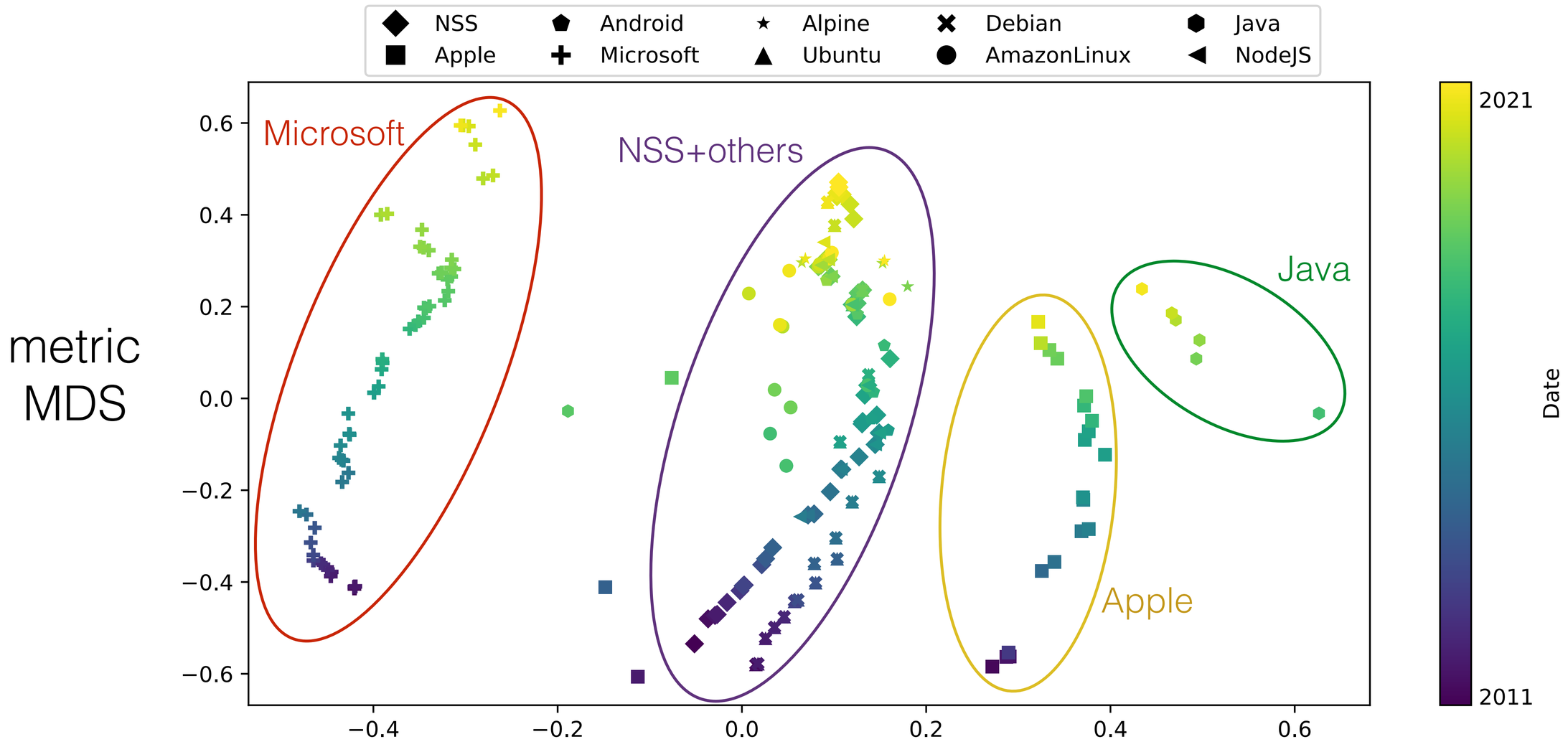
4. How faithfully do providers copy root program trust?

Clustering providers

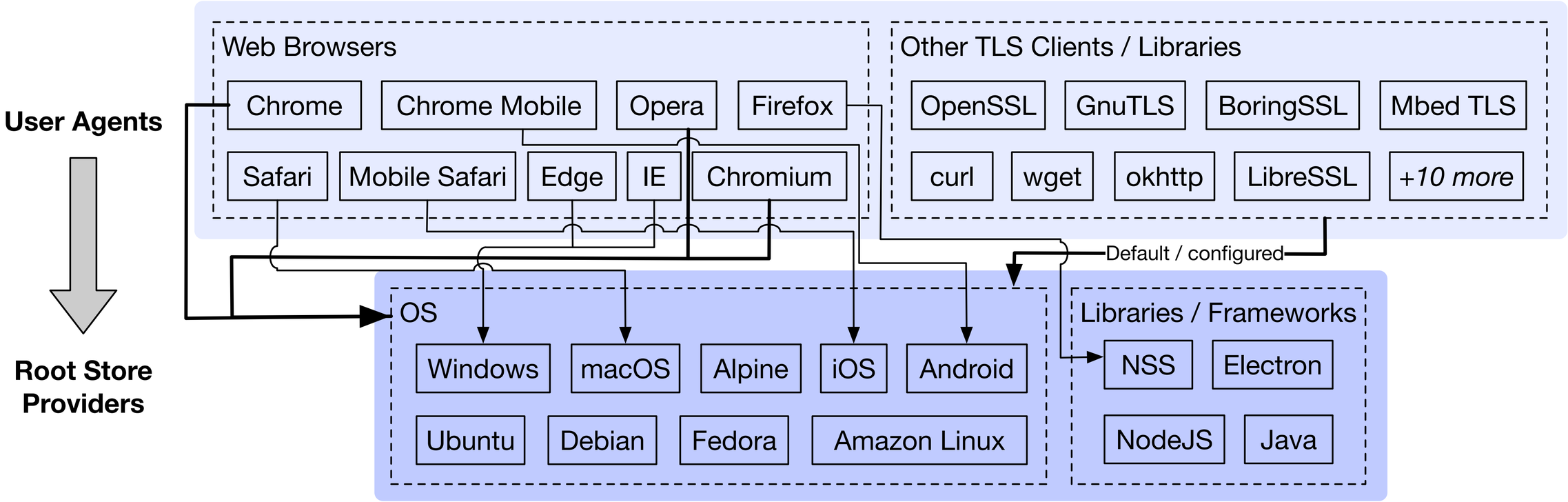
metric MDS



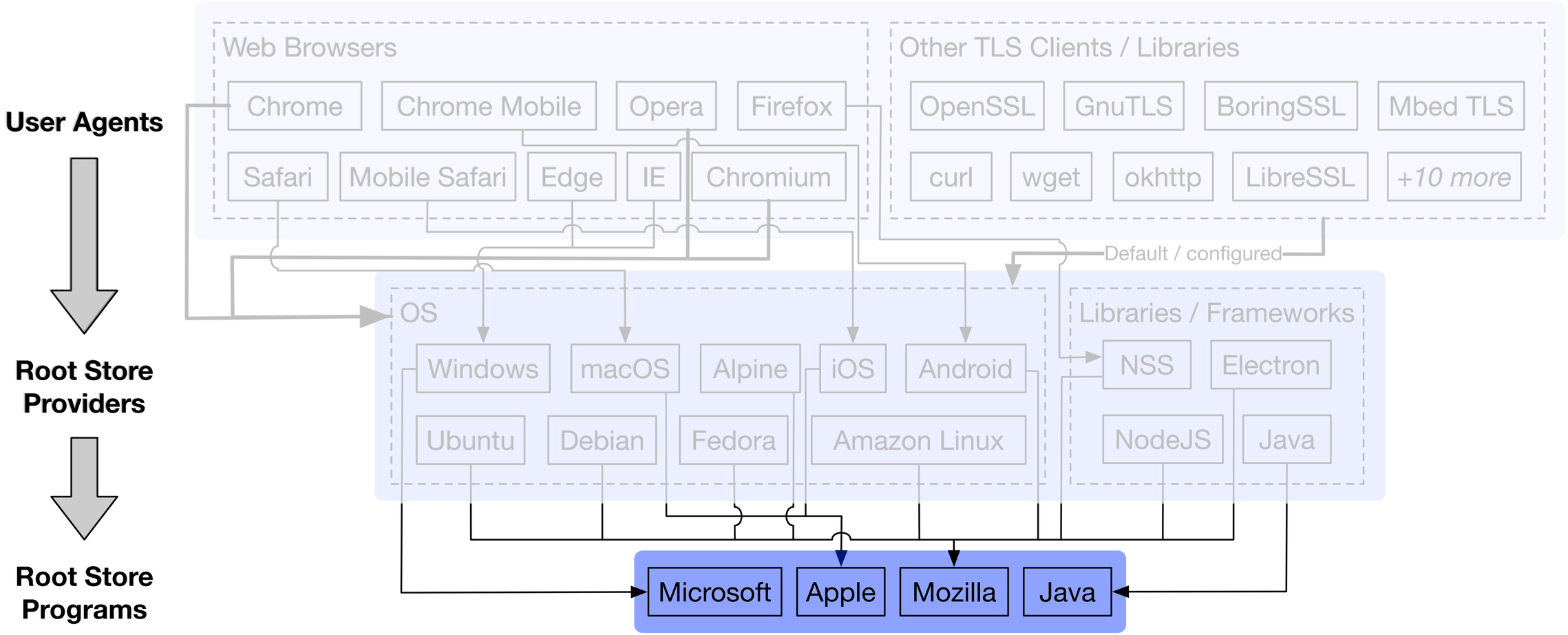
Clustering providers



Root store providers



Root store programs



Research Questions

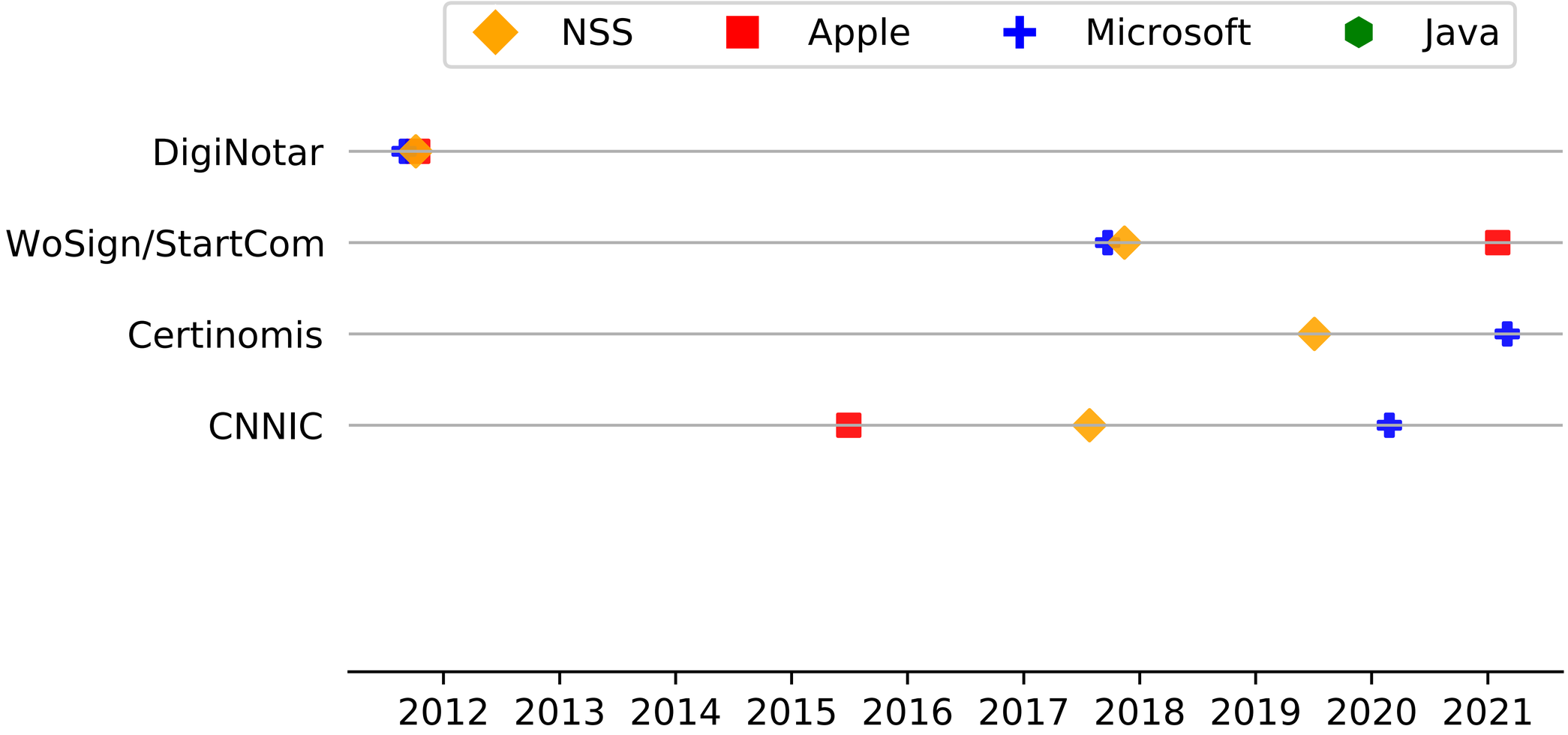
1. Which root store providers do TLS user agents rely on?

2. How do root store providers determine which CAs to trust?

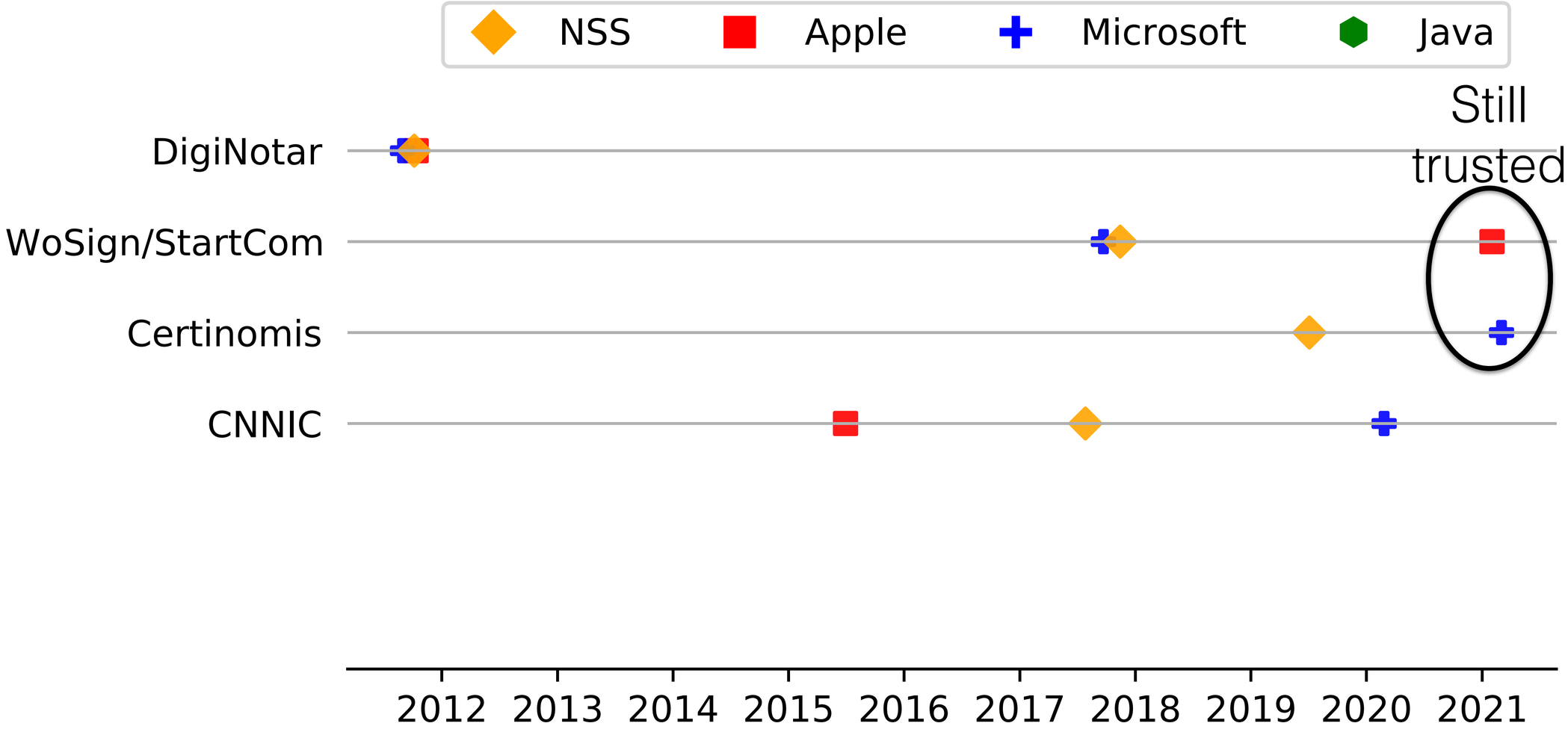
3. Characterization of root store programs

4. How faithfully do providers copy root program trust?

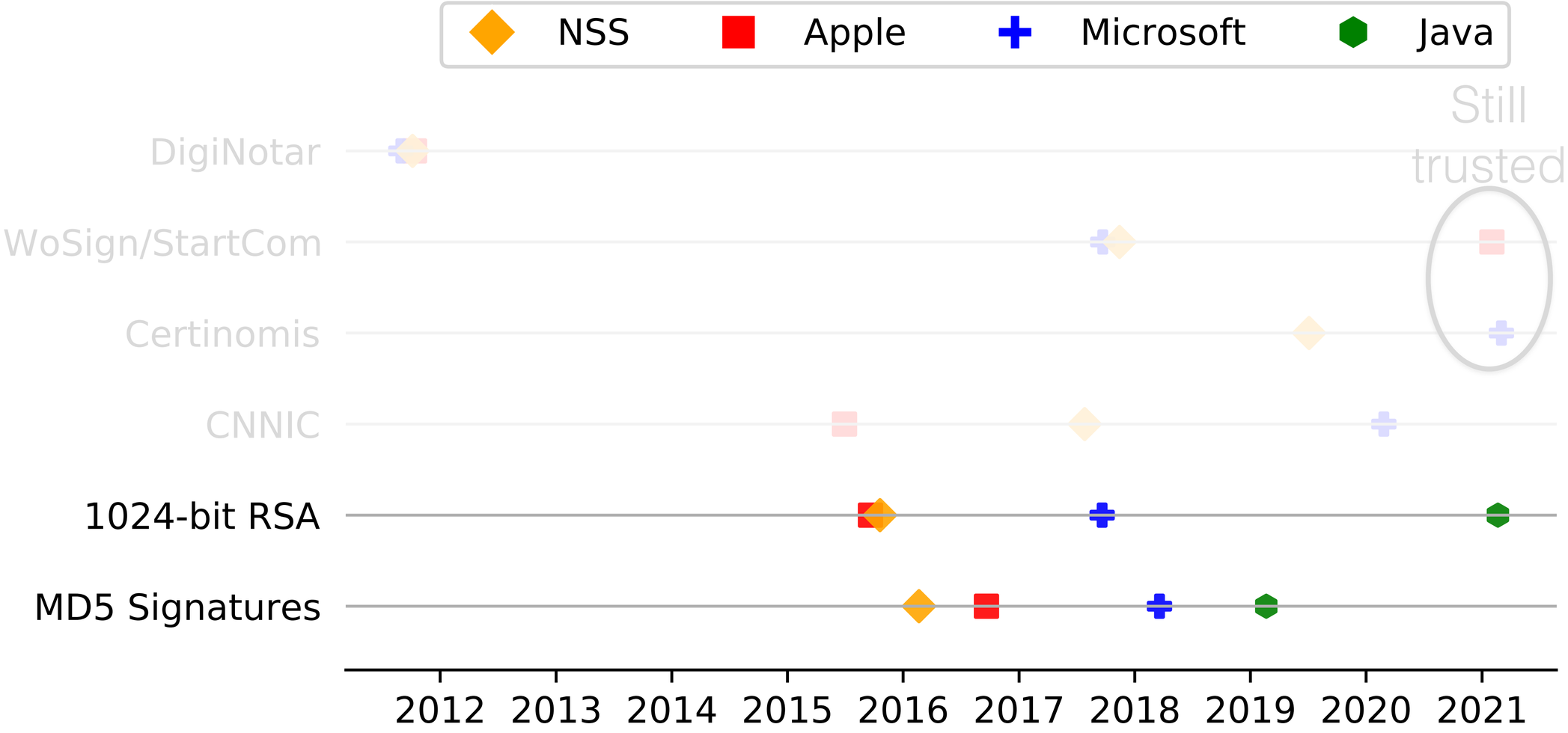
Root program comparison



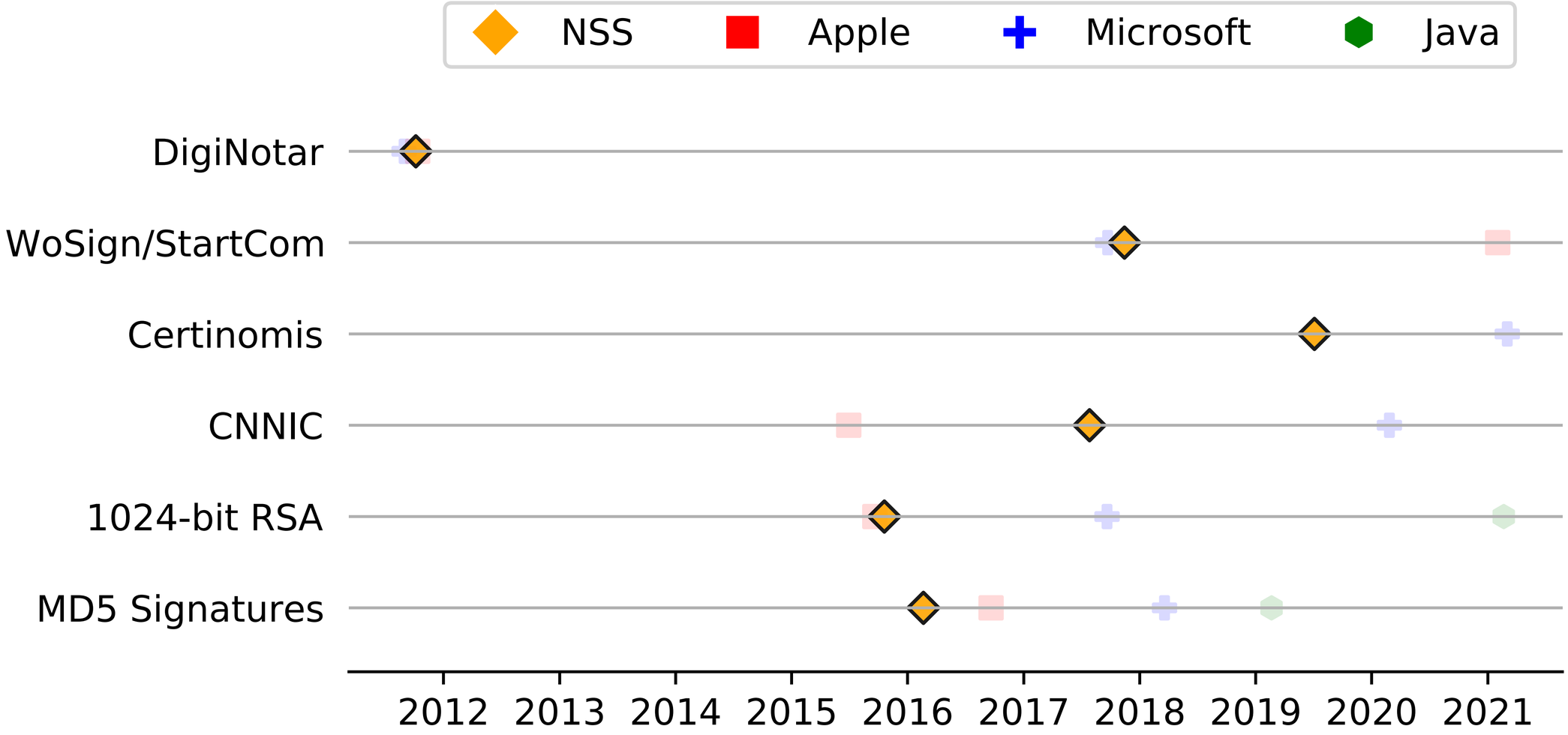
Root program comparison



Root program comparison



Root program comparison



Root program comparison

1. Mozilla responds quickly to CA distrust incidents; Microsoft relatively slow, Apple varies.

2. Apple/Mozilla operate relatively hygienic root stores.

Root program comparison

1. Mozilla responds quickly to CA distrust incidents; Microsoft relatively slow, Apple varies.

2. Apple/Mozilla operate relatively hygienic root stores.

3. Size: Mozilla < Apple < Microsoft; Mozilla most restrictive, Microsoft allows government super-CAs.

Root program comparison

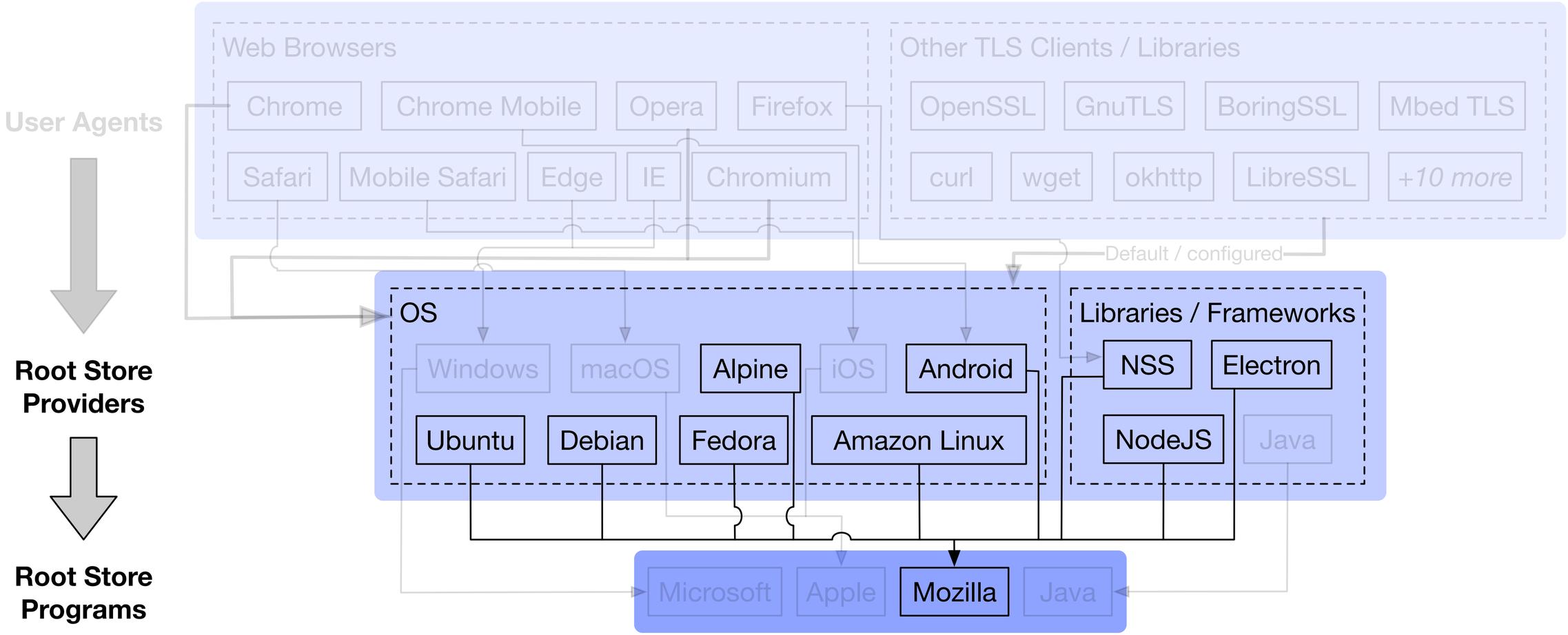
1. Mozilla responds quickly to CA distrust incidents; Microsoft relatively slow, Apple varies.

2. Apple/Mozilla operate relatively hygienic root stores.

3. Size: Mozilla < Apple < Microsoft; Mozilla most restrictive, Microsoft allows government super-CAs.

4. Mozilla runs the most transparent root store program.

Mozilla derivatives



Research Questions

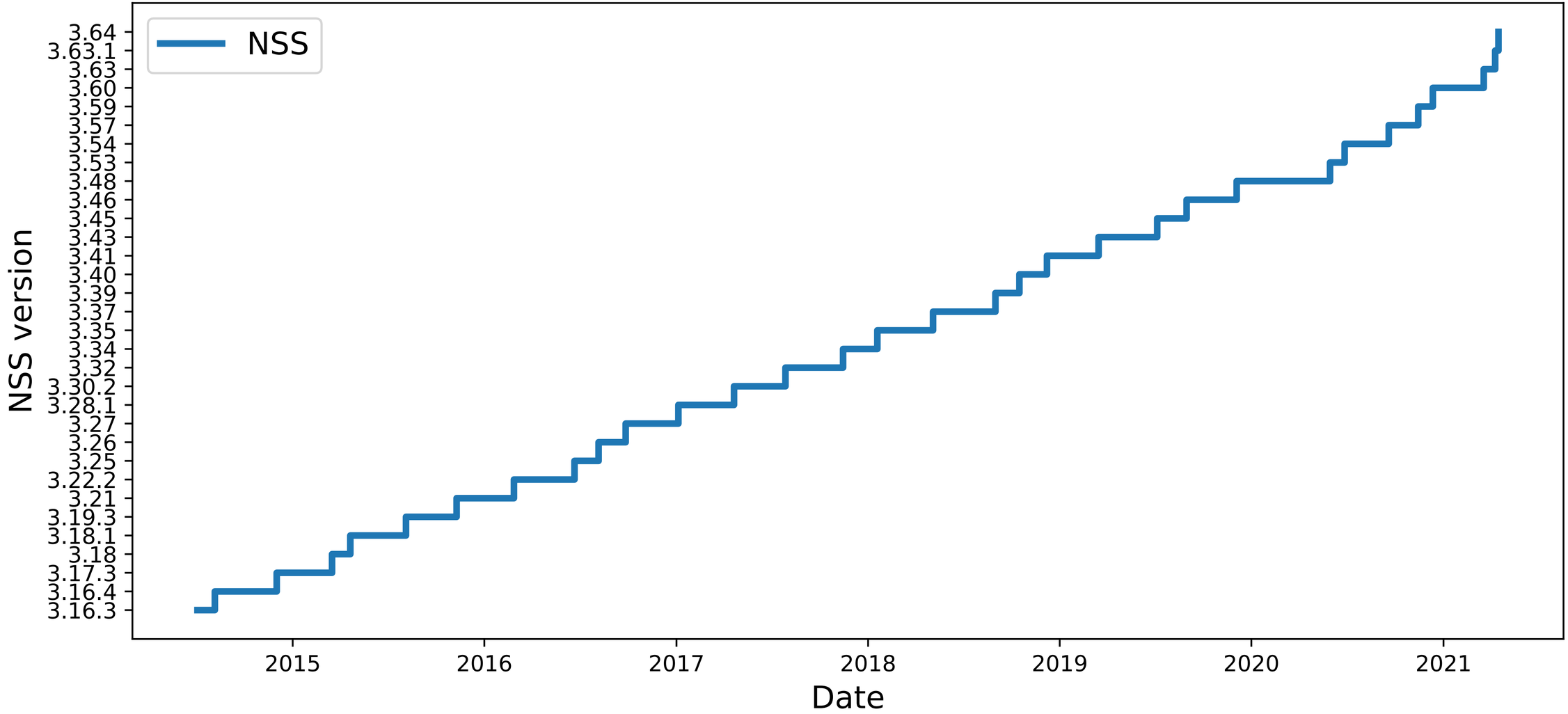
1. Which root store providers do TLS user agents rely on?

2. How do root store providers determine which CAs to trust?

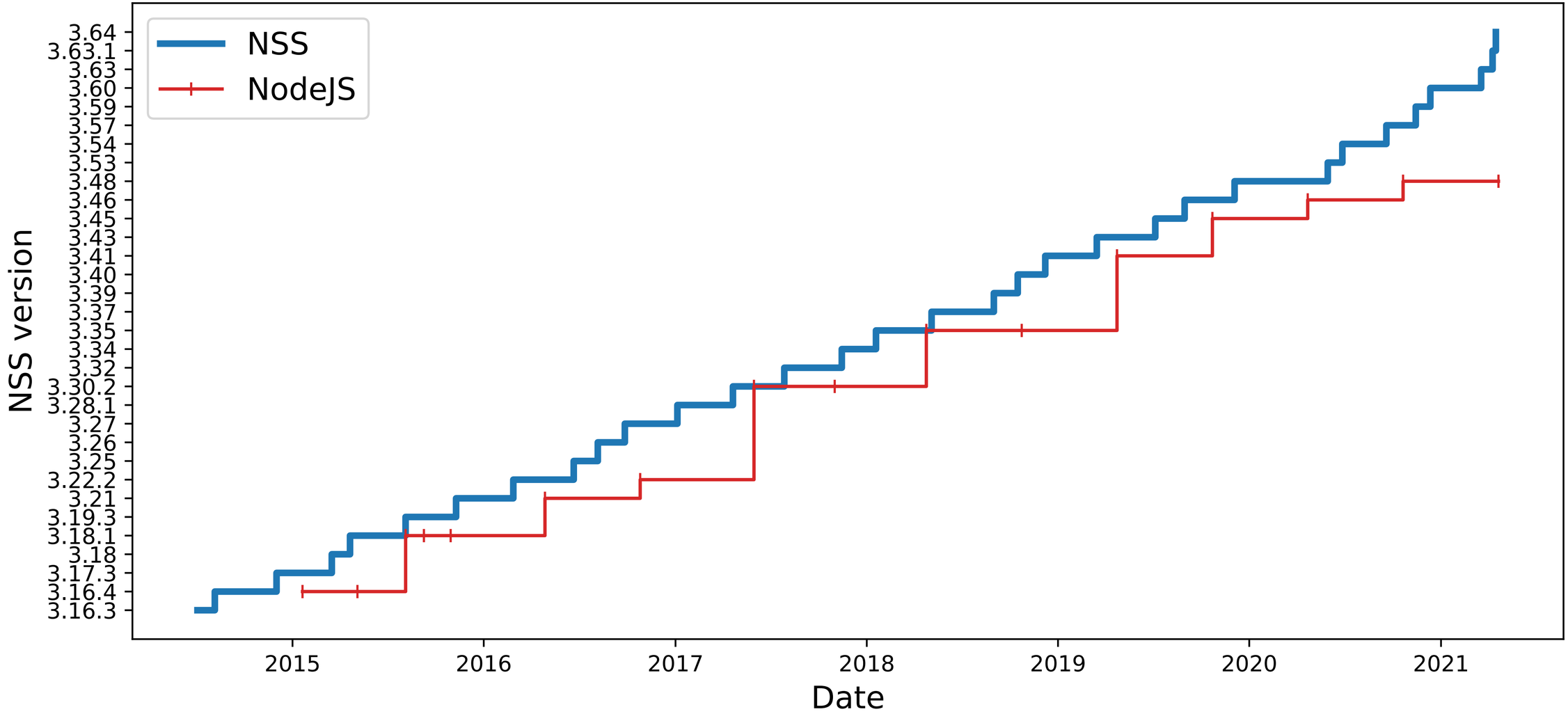
3. Characterization of root store programs

4. How faithfully do providers copy root program trust?

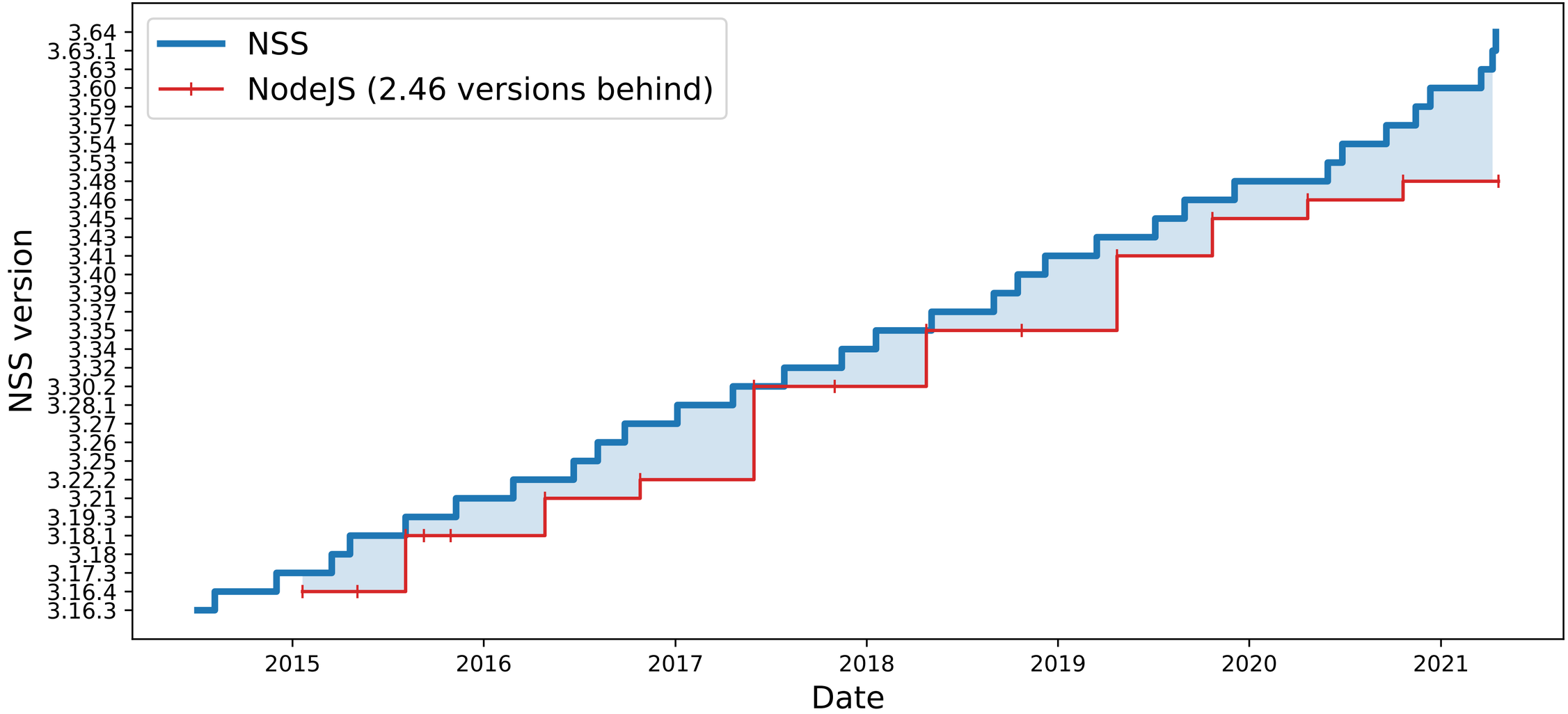
Derivative delay



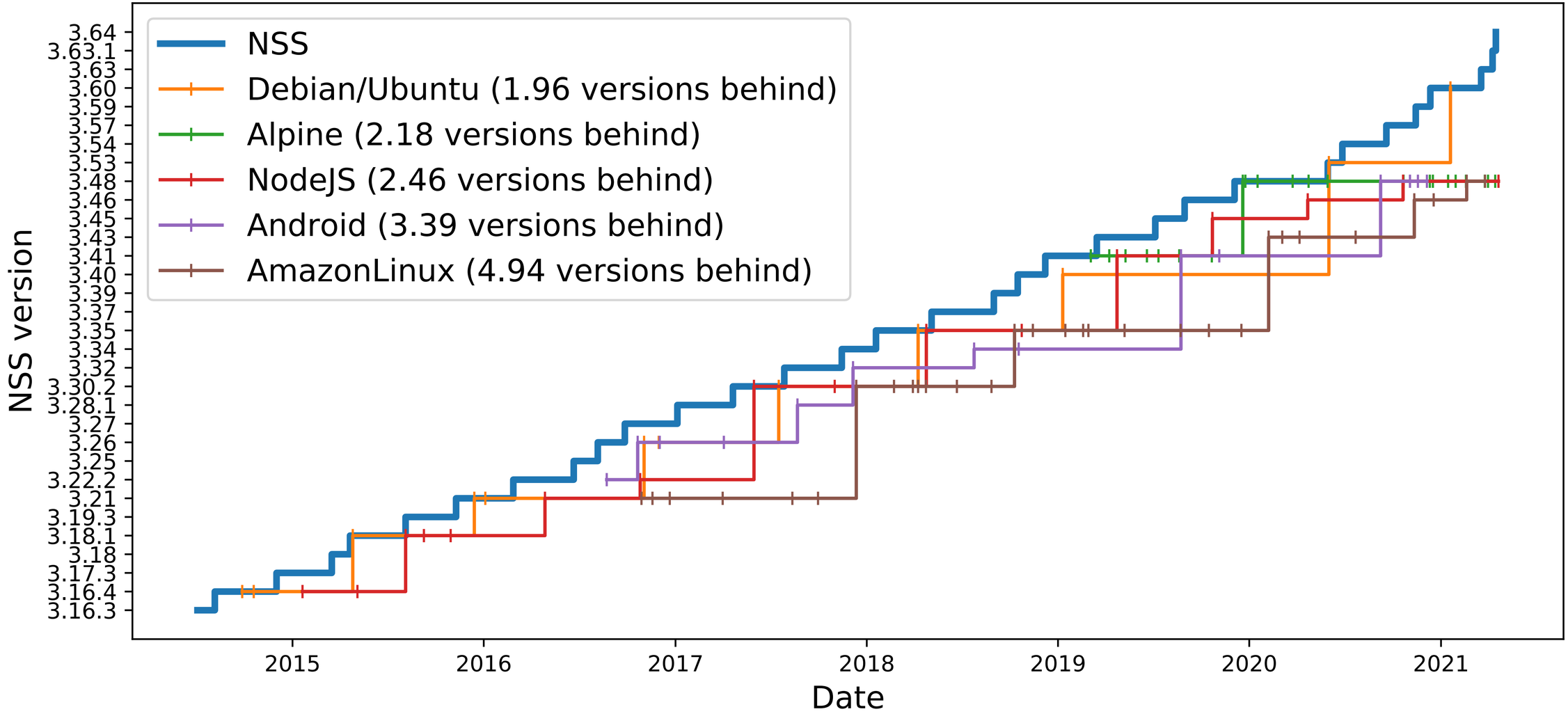
Derivative delay



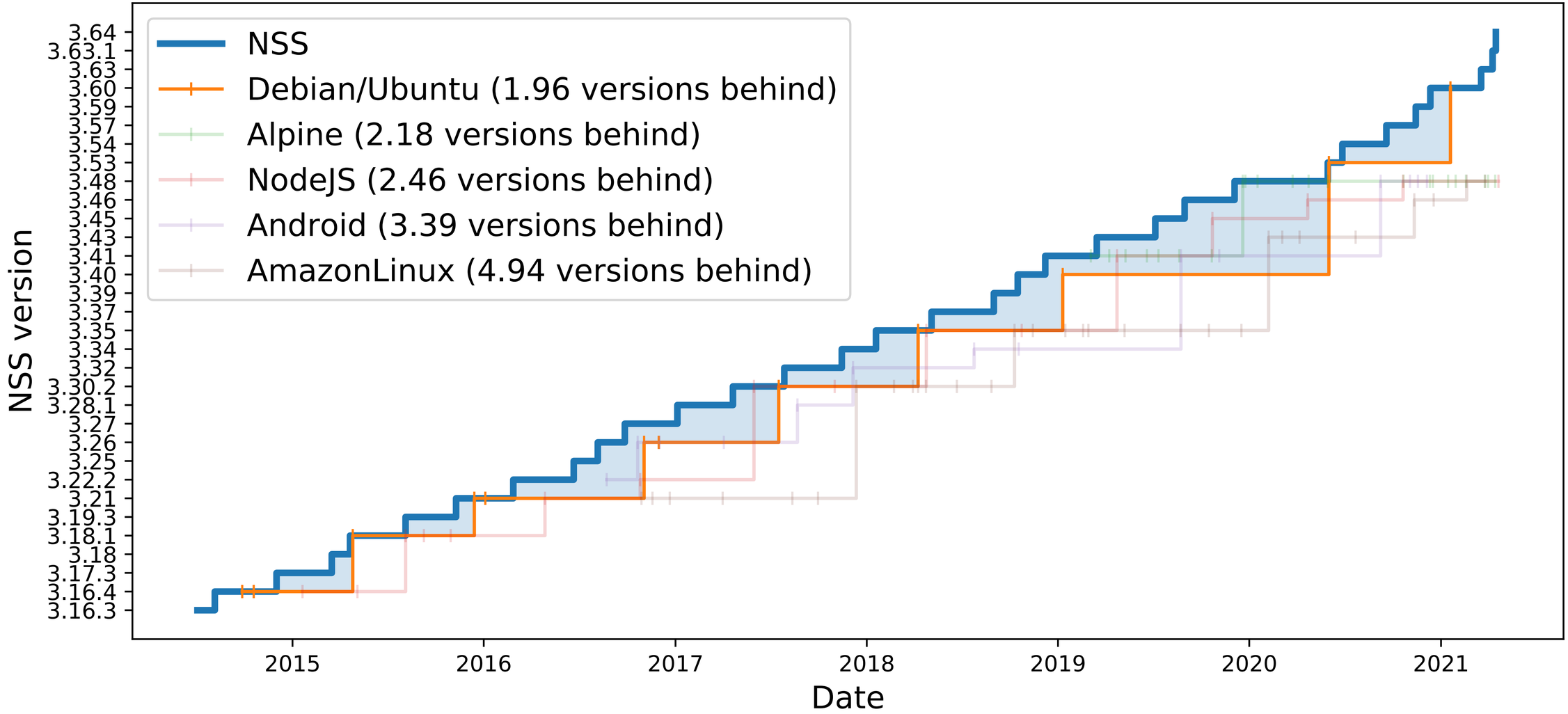
Derivative delay



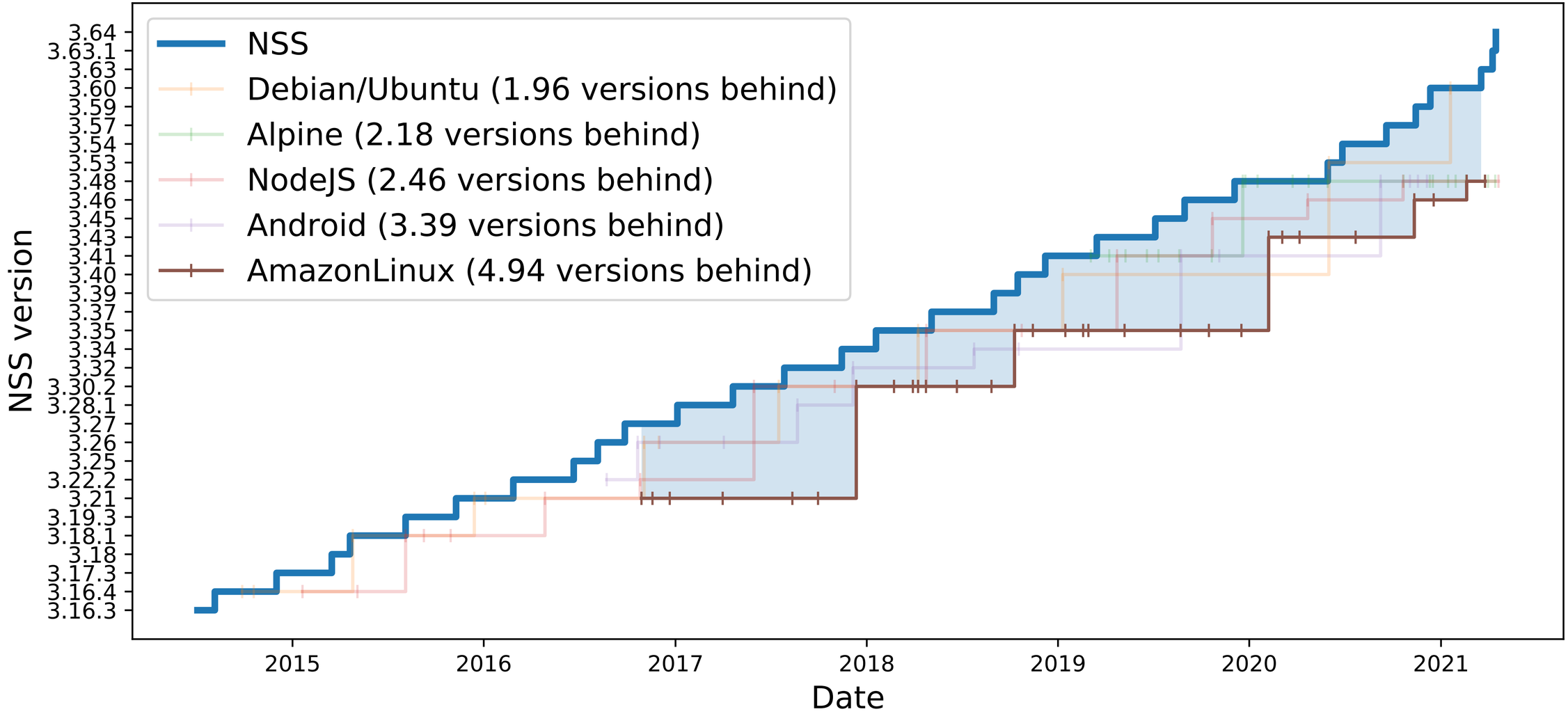
Derivative delay



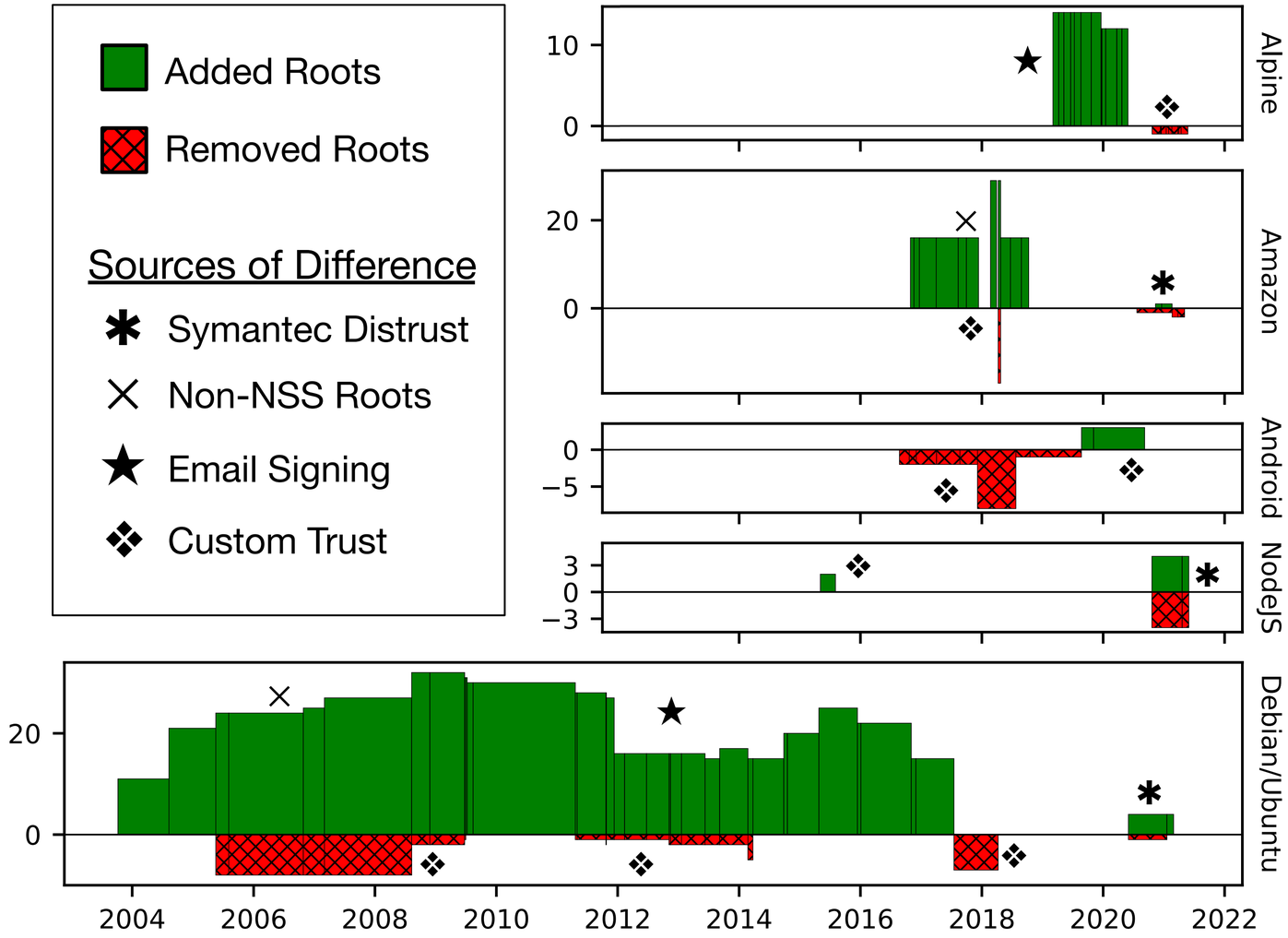
Derivative delay



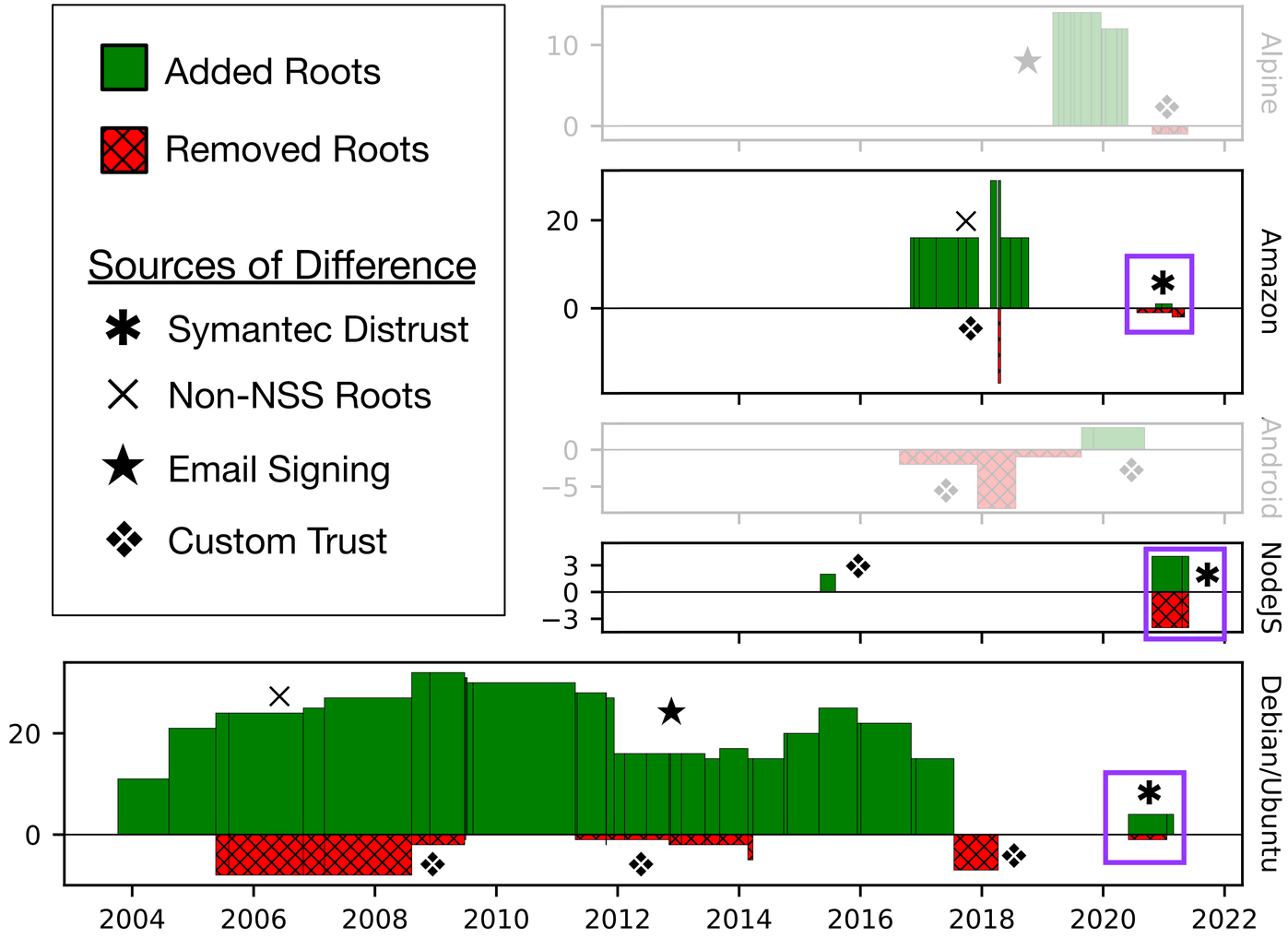
Derivative delay



Trust deviations



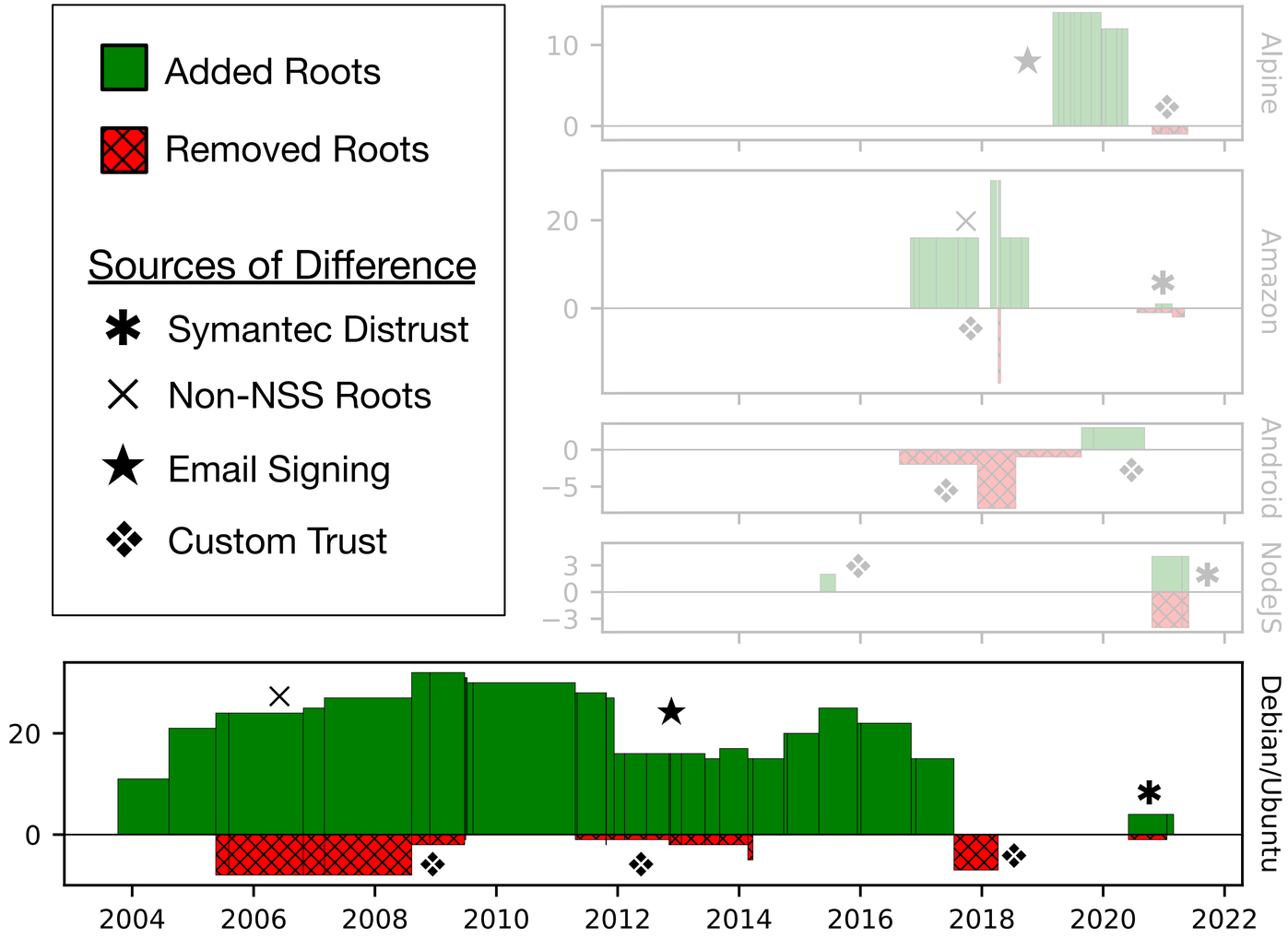
Trust deviations



Trust purpose conflation: trusting non-TLS certificates

Partial trust incapability: Symantec distrust dilemma

Trust deviations



Trust purpose conflation: trusting non-TLS certificates

Partial trust incapability: Symantec distrust dilemma

Non-NSS trusted CAs: questionable trust

App. developer confusion: trusting CAs for code signing, timestamping

Summary

Popular TLS user agents infrequently make their own TLS trust decisions and rely on the OS.

Apple, Microsoft run major root programs; all other root providers originate from Mozilla's NSS root program.

Summary

Popular TLS user agents infrequently make their own TLS trust decisions and rely on the OS.

Apple, Microsoft run major root programs; all other root providers originate from Mozilla's NSS root program.

NSS derivatives copy poorly: delayed updates, questionable bespoke trust, incompatible trust scope.

Summary

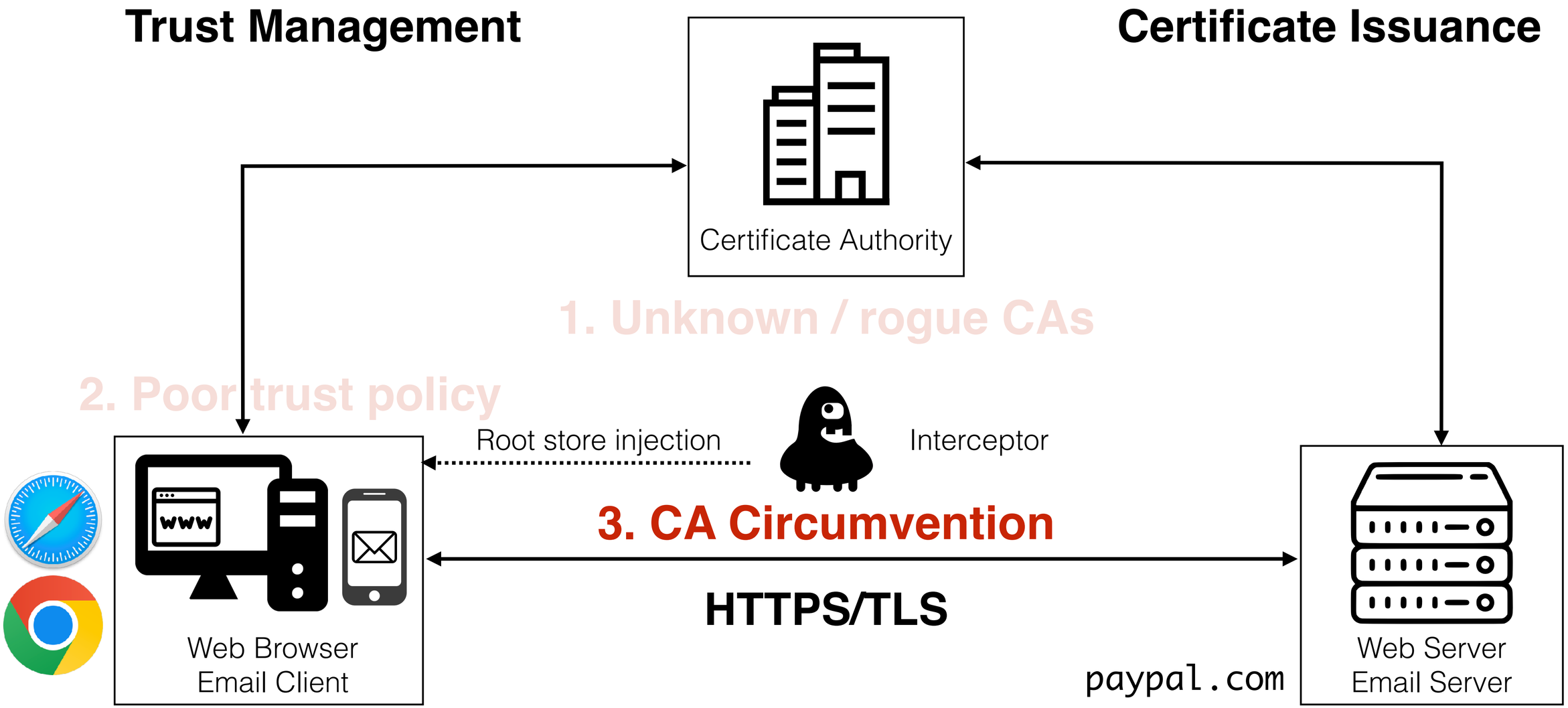
Popular TLS user agents infrequently make their own TLS trust decisions and rely on the OS.

Apple, Microsoft run major root programs; all other root providers originate from Mozilla's NSS root program.

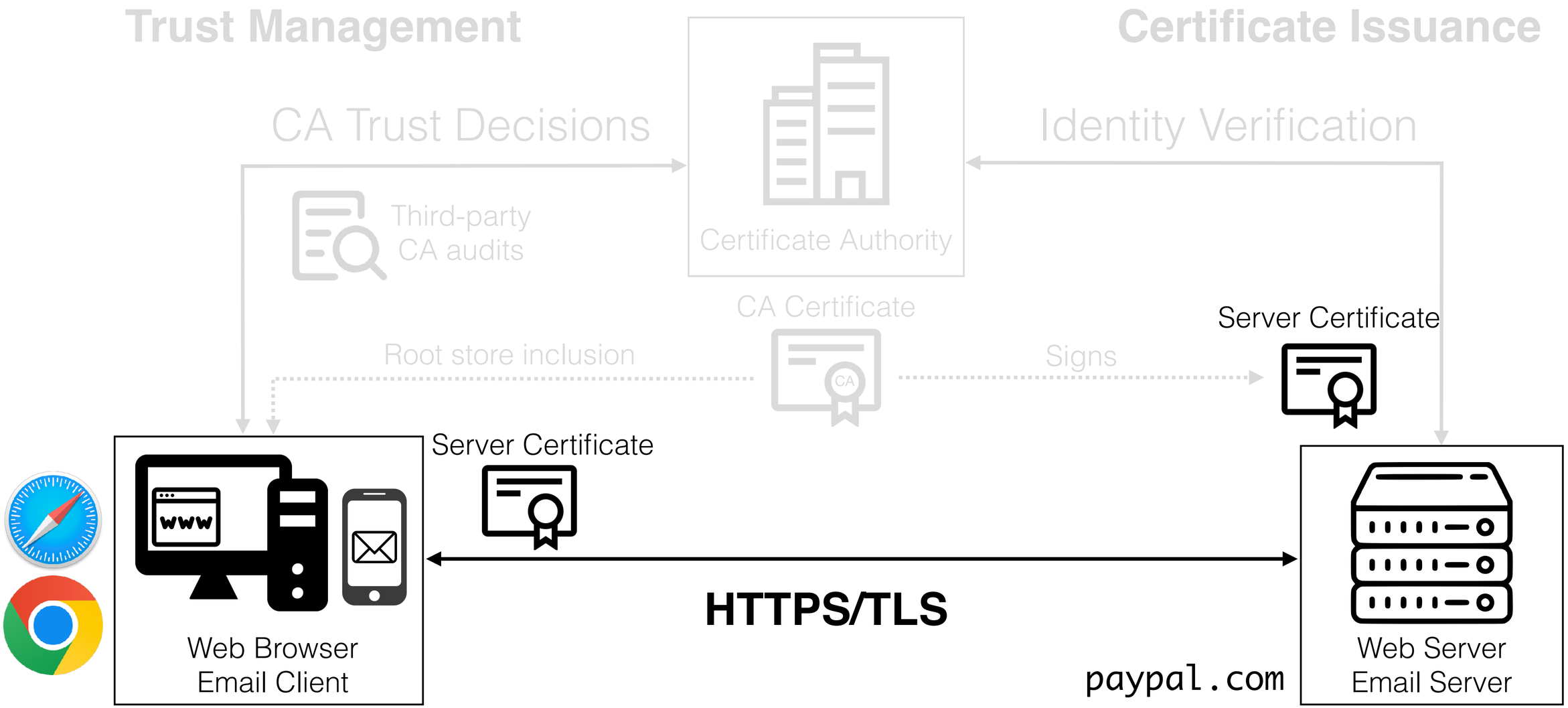
NSS derivatives copy poorly: delayed updates, questionable bespoke trust, incompatible trust scope.

Explicit provenance transparency and consistent trust schema would reduce manual copying, spotlight questionable custom trust.

Roadmap

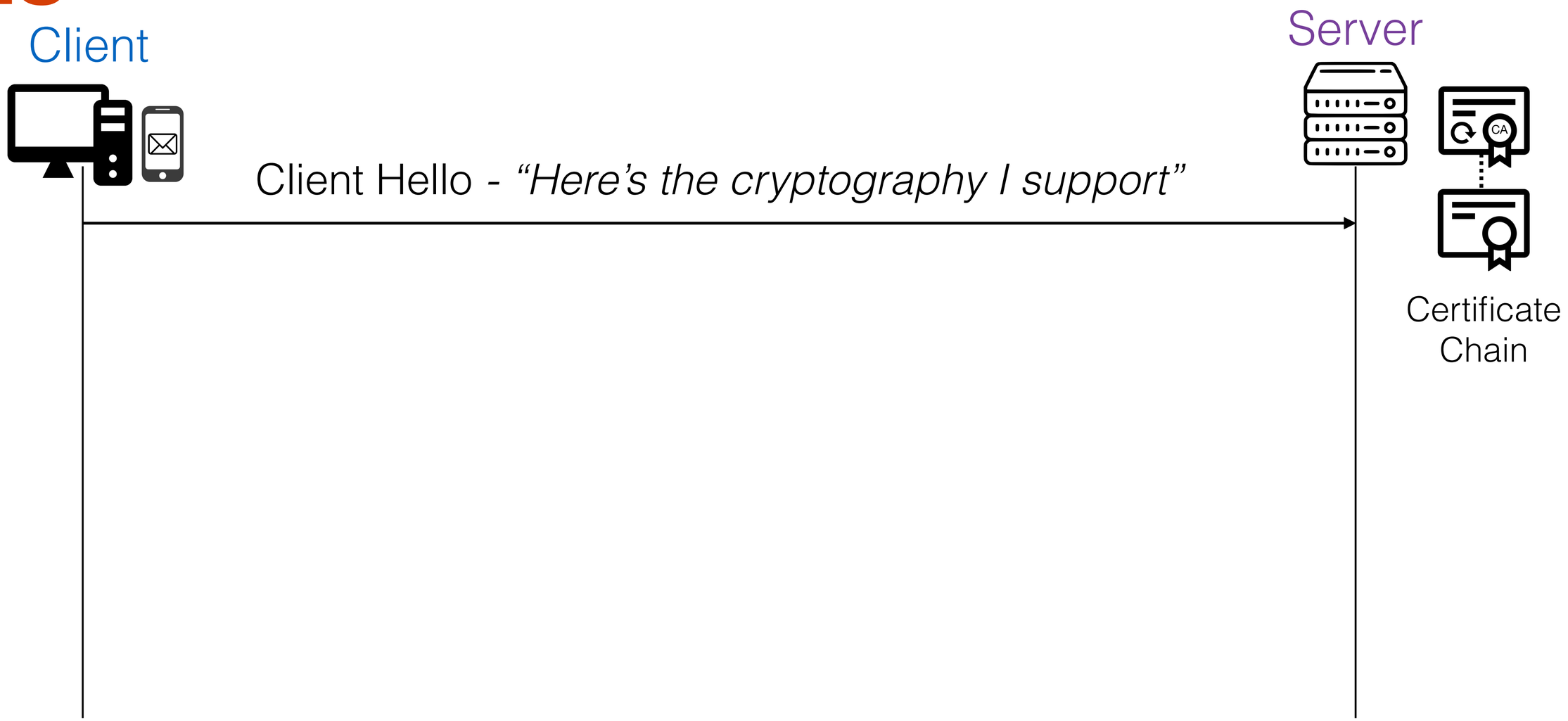

Trust Management
Certificate Issuance
Certificate Authority
1. Unknown / rogue CAs
2. Poor trust policy
Root store injection
Interceptor
3. CA Circumvention
HTTPS/TLS
Web Browser
Email Client
paypal.com
Web Server
Email Server

TLS

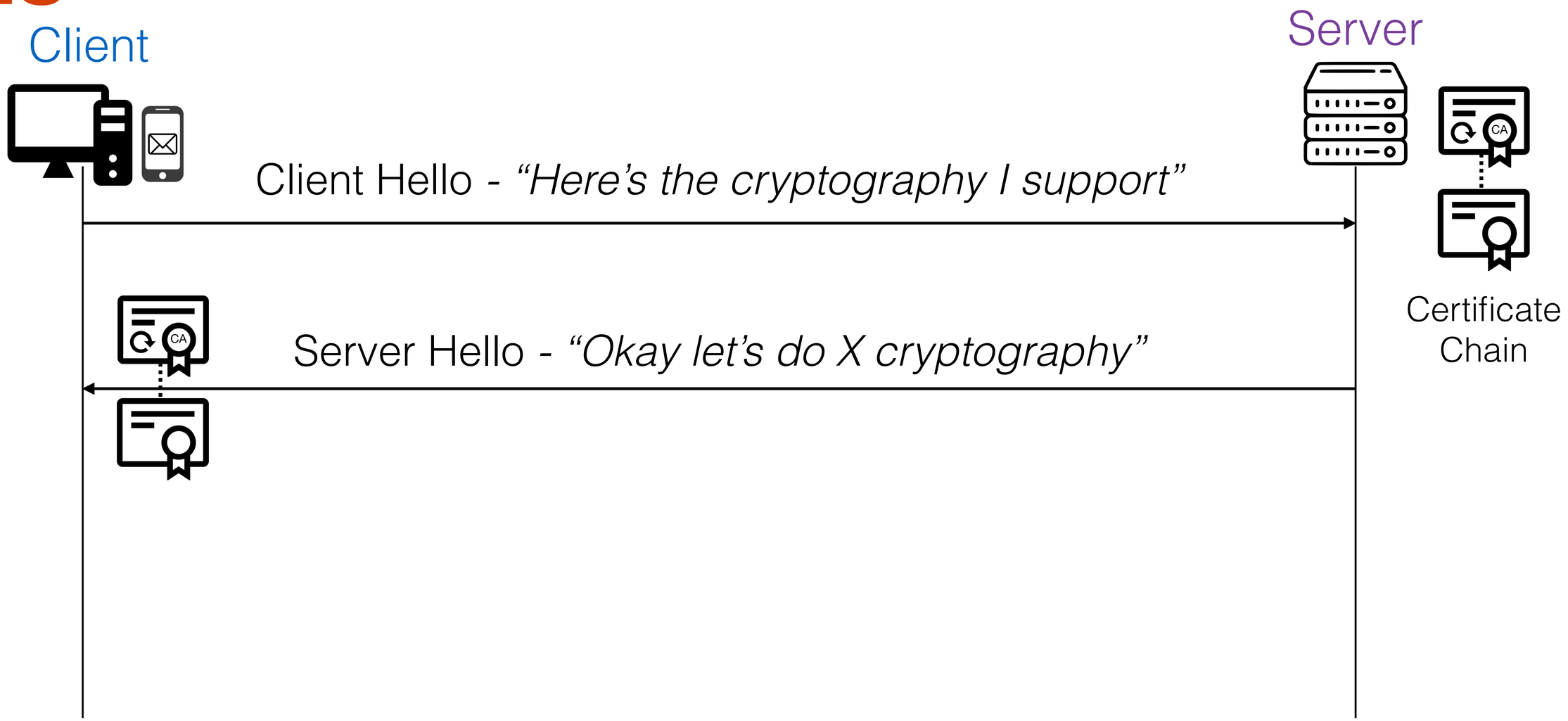

Trust Management
Certificate Issuance
CA Trust Decisions
Identity Verification
Third-party
CA audits
Certificate Authority
CA Certificate
Server Certificate
Root store inclusion
Signs
CA
Server Certificate
www
Web Browser
Email Client
HTTPS/TLS
paypal.com
Web Server
Email Server

TLS

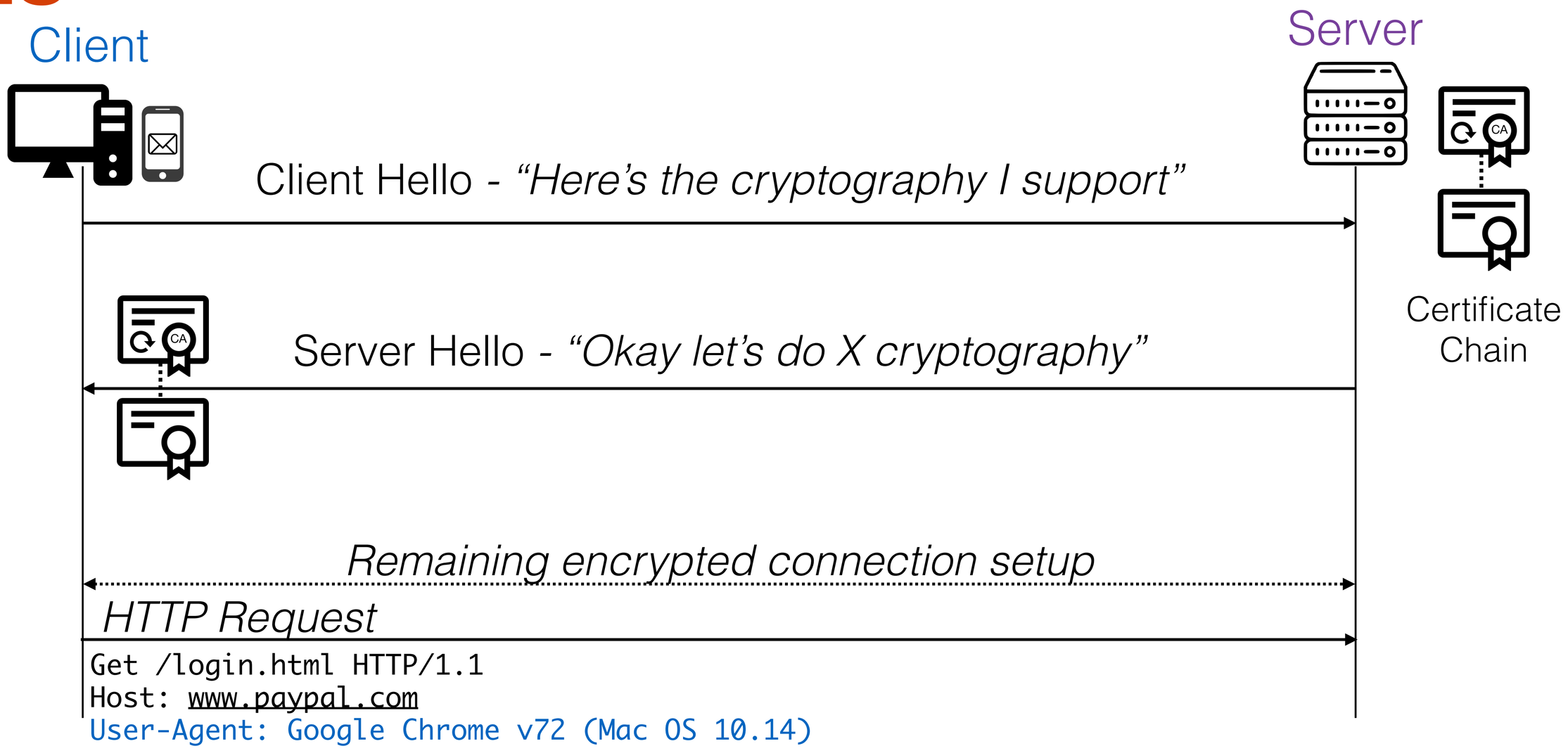
TLS


Client
Server
Client Hello - *"Here's the cryptography I support"*
CA
Certificate Chain

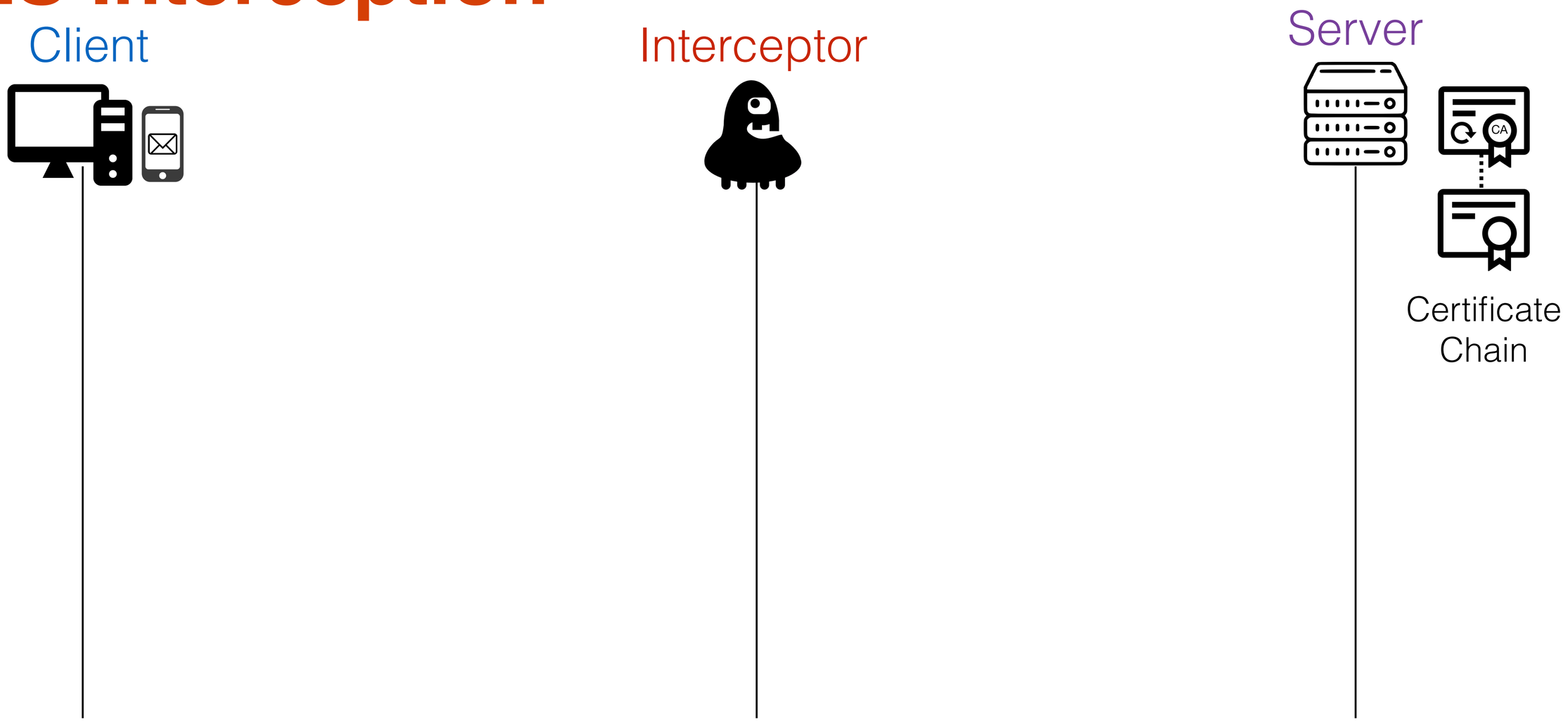
TLS


Client
Server
Client Hello - *"Here's the cryptography I support"*
Server Hello - *"Okay let's do X cryptography"*
CA
CA
Certificate Chain

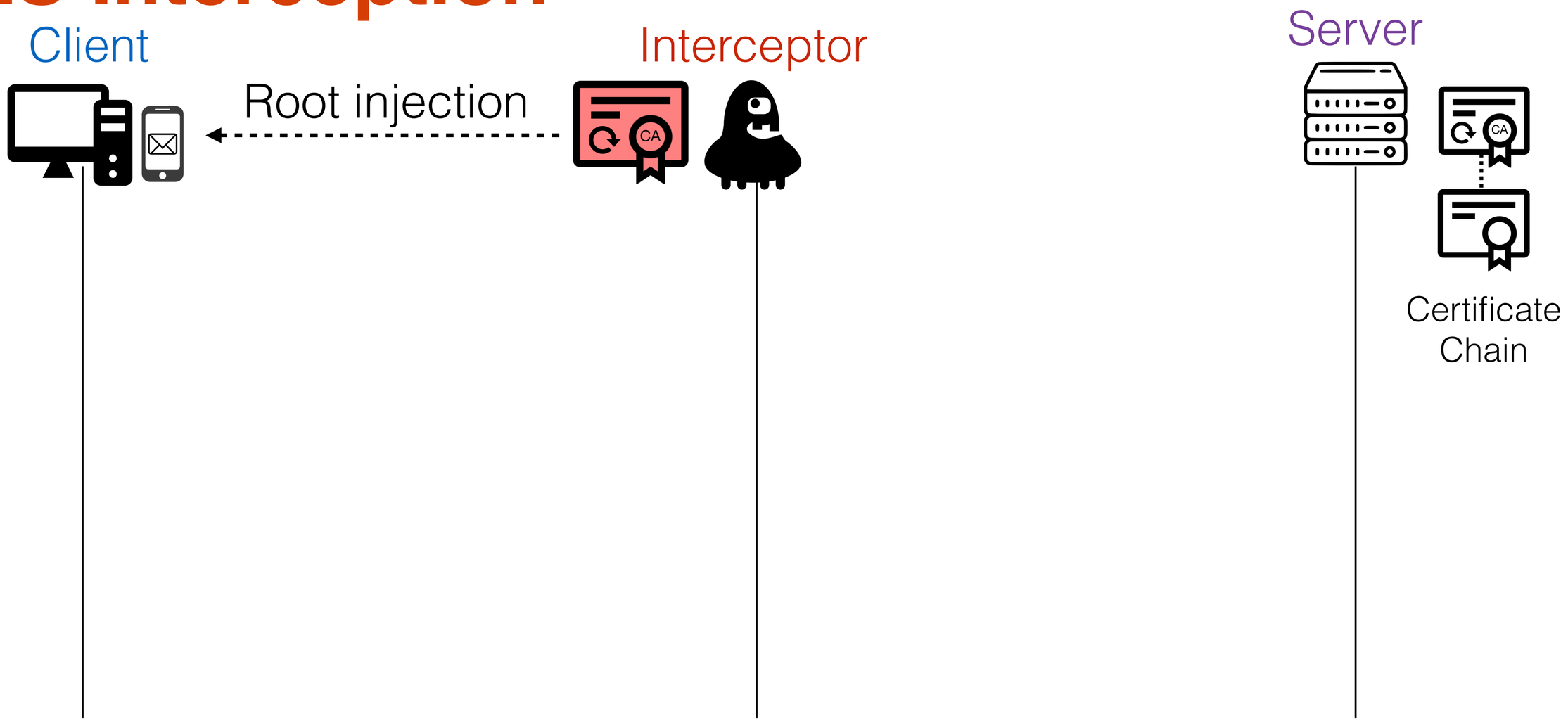
TLS


Client
Server
Client Hello - *"Here's the cryptography I support"*
Certificate Chain
Server Hello - *"Okay let's do X cryptography"*
Remaining encrypted connection setup
HTTP Request
Get /login.html HTTP/1.1
Host: www.paypal.com
User-Agent: Google Chrome v72 (Mac OS 10.14)

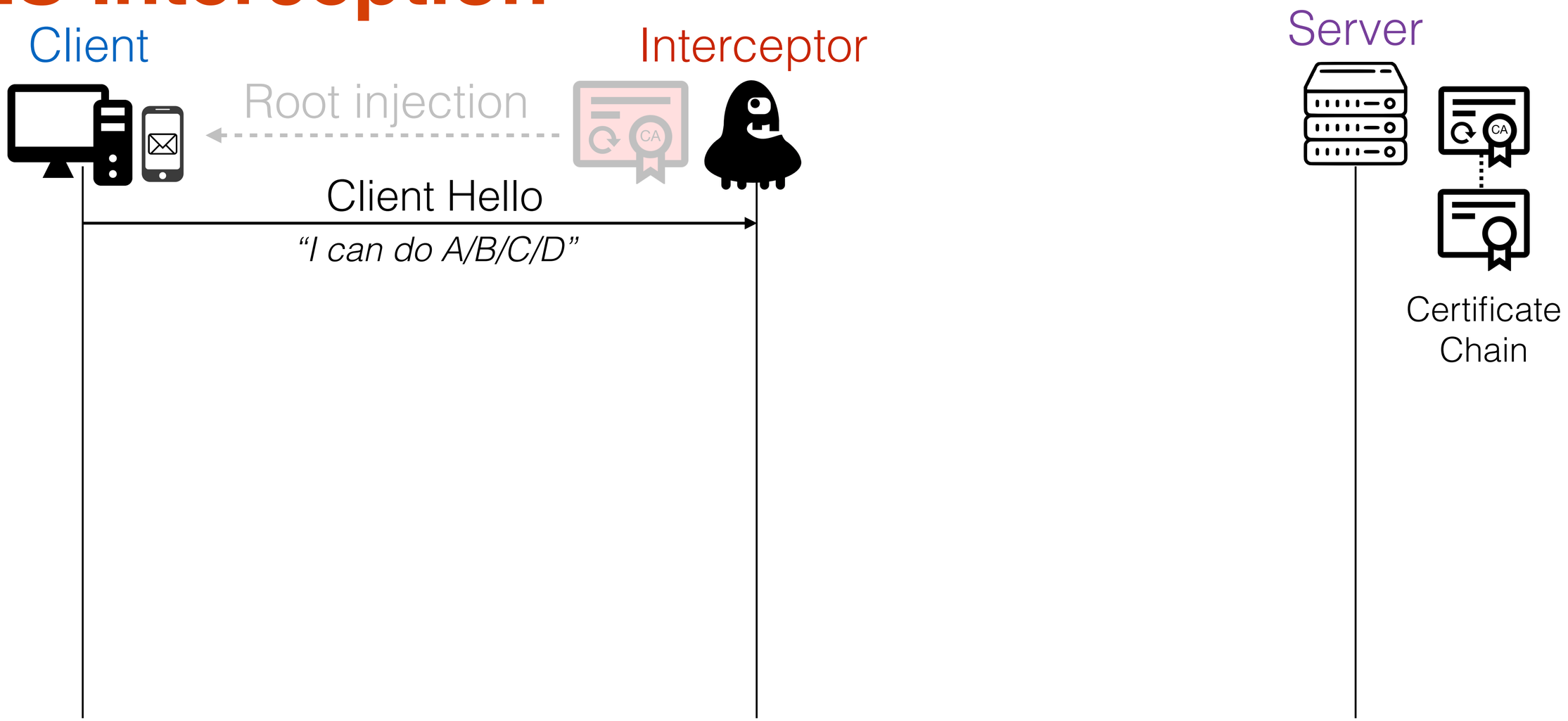
TLS Interception



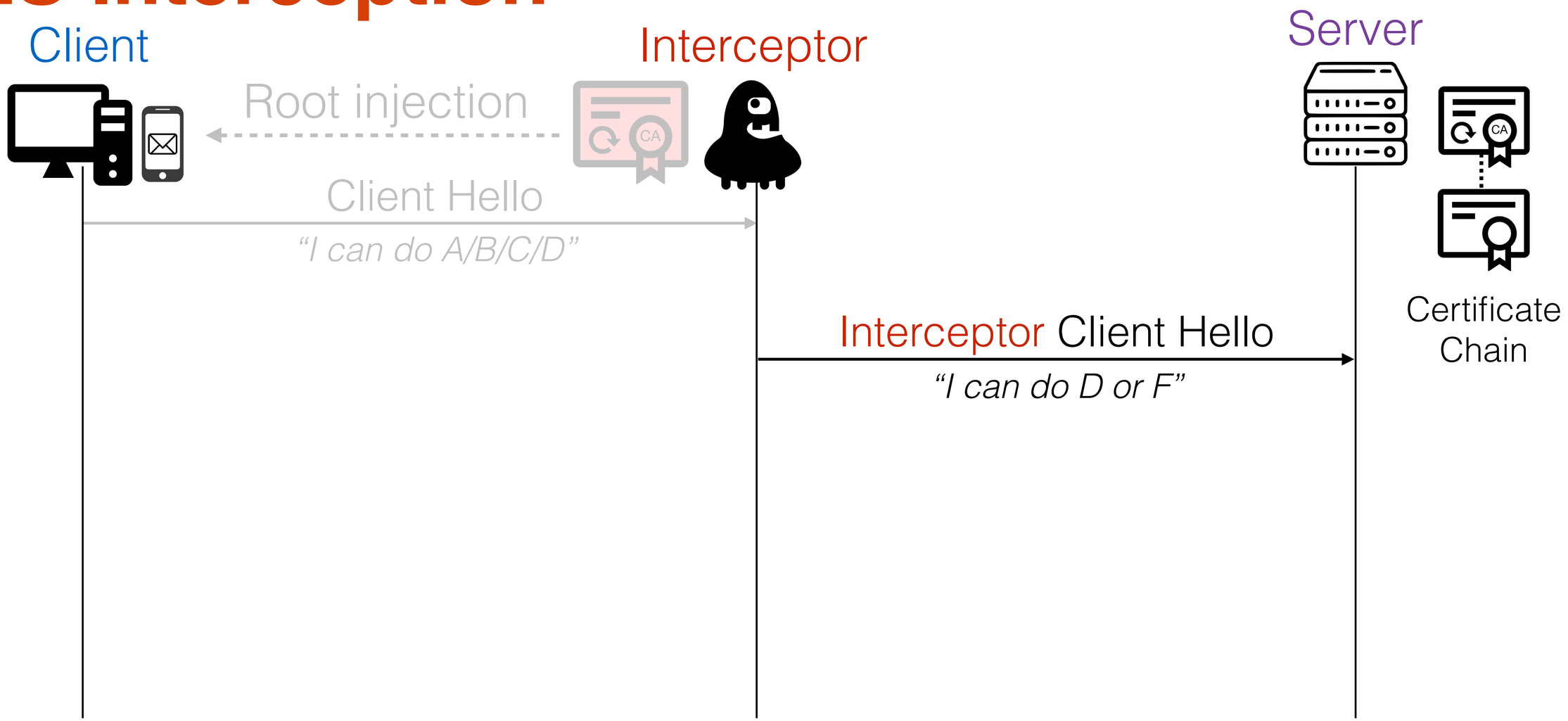
TLS Interception



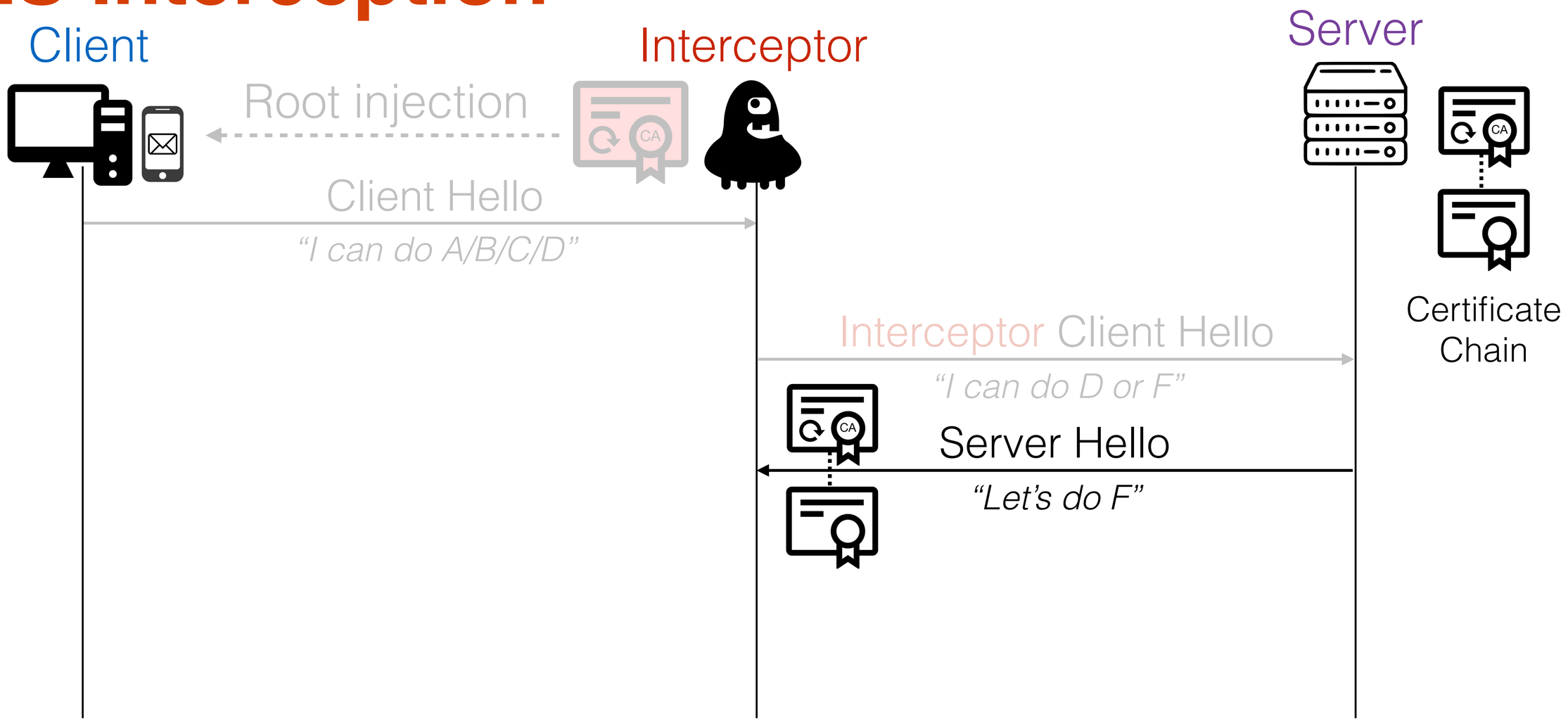
TLS Interception



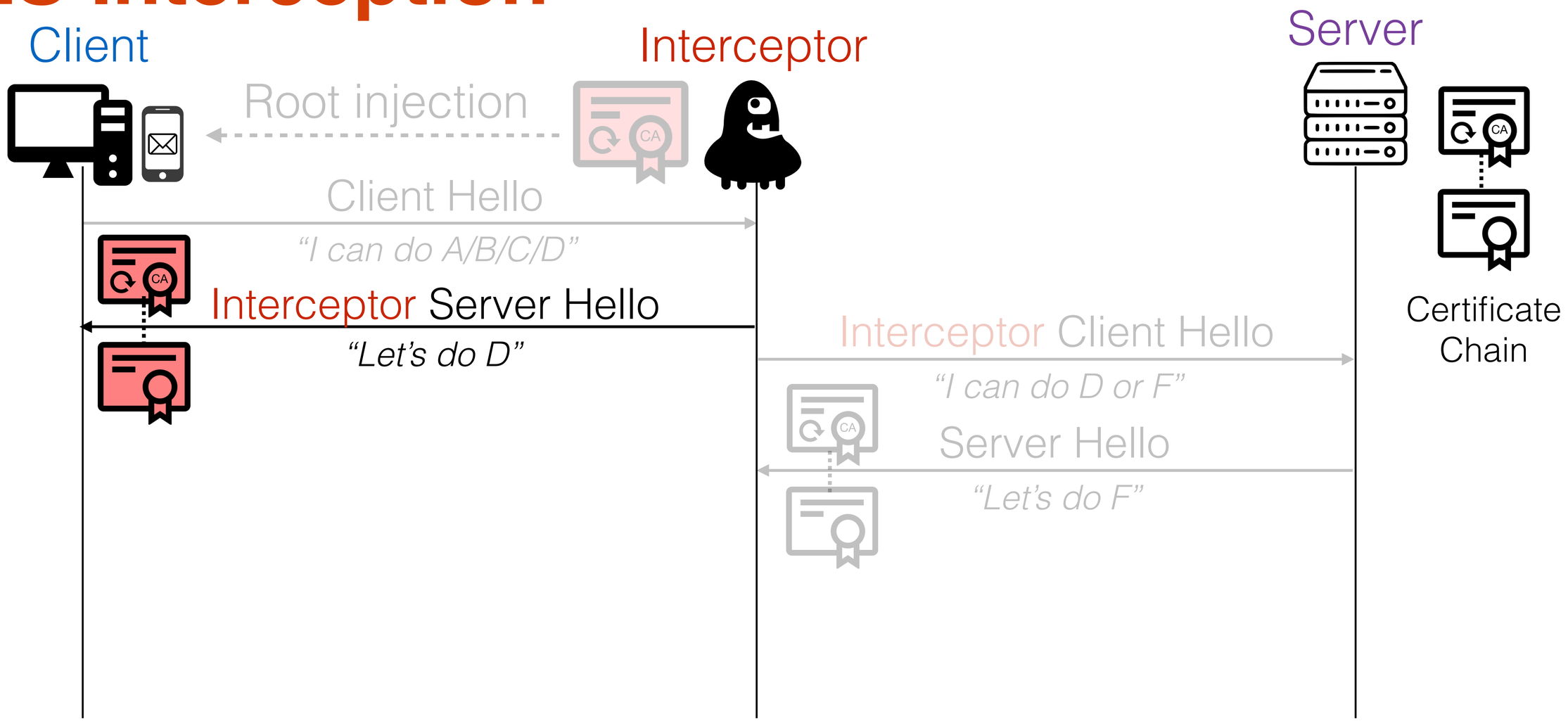
TLS Interception



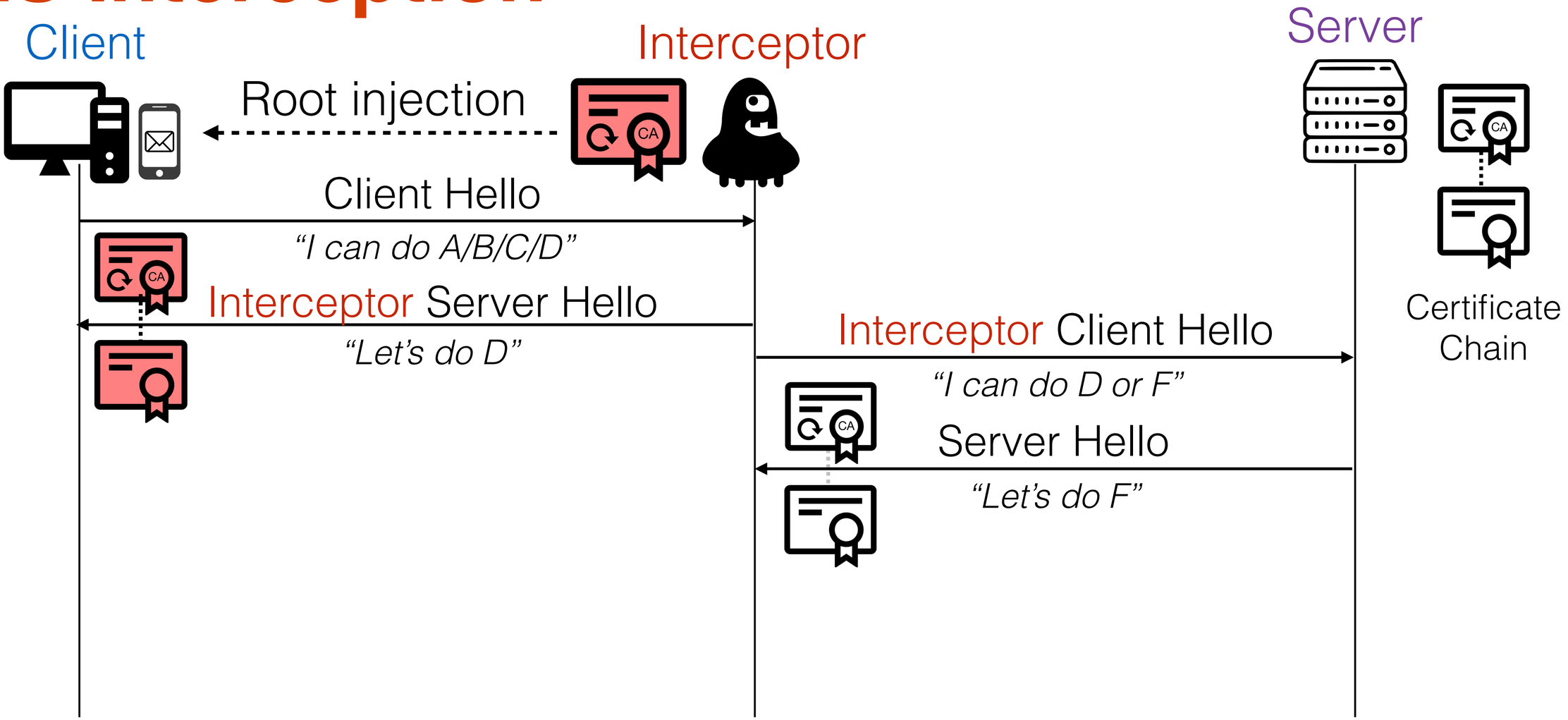
TLS Interception



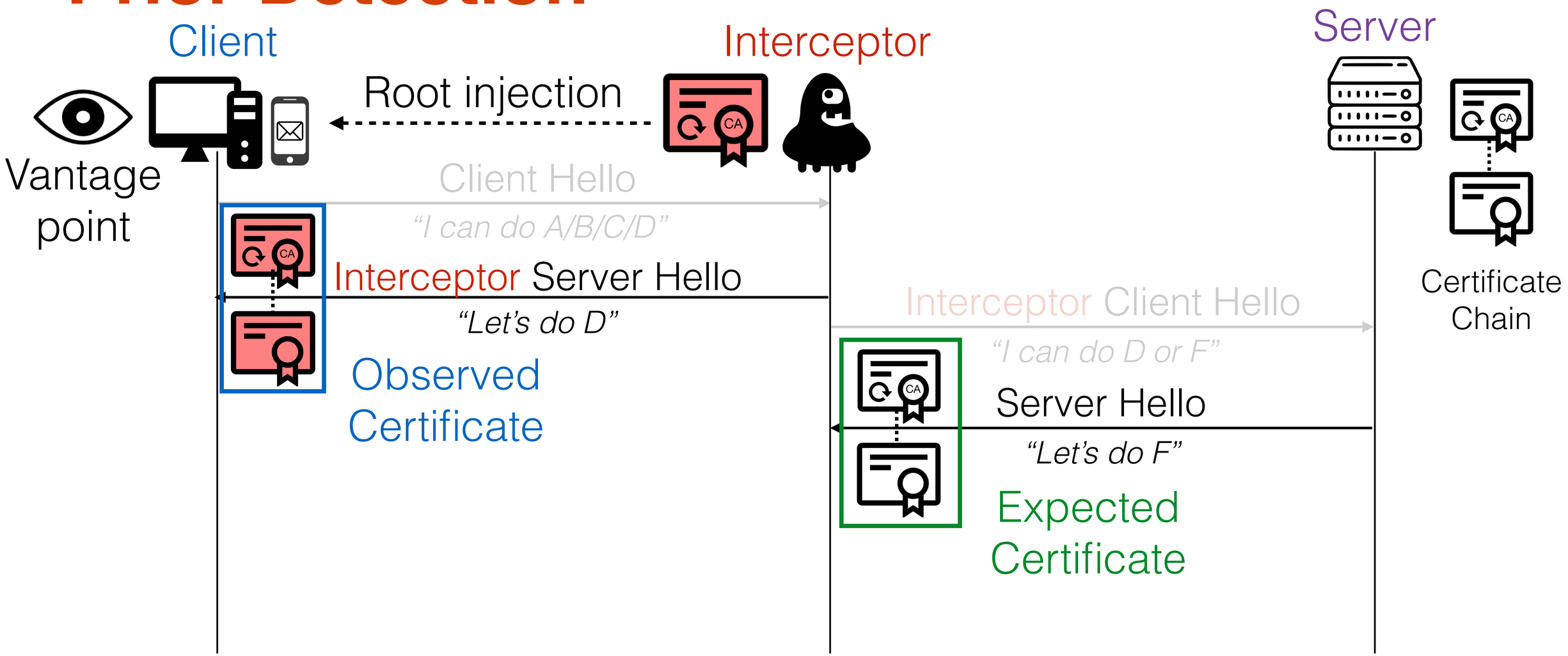
TLS Interception



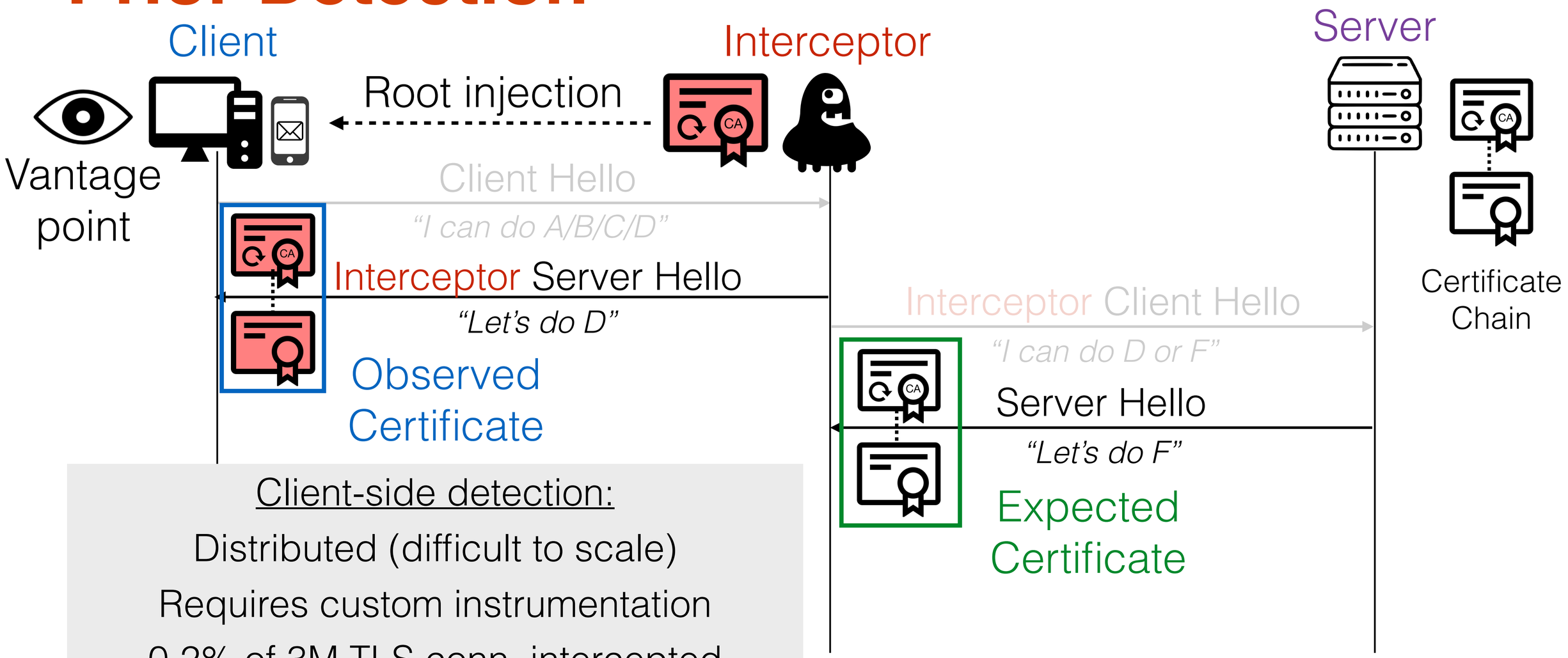
TLS Interception



Prior Detection



Prior Detection



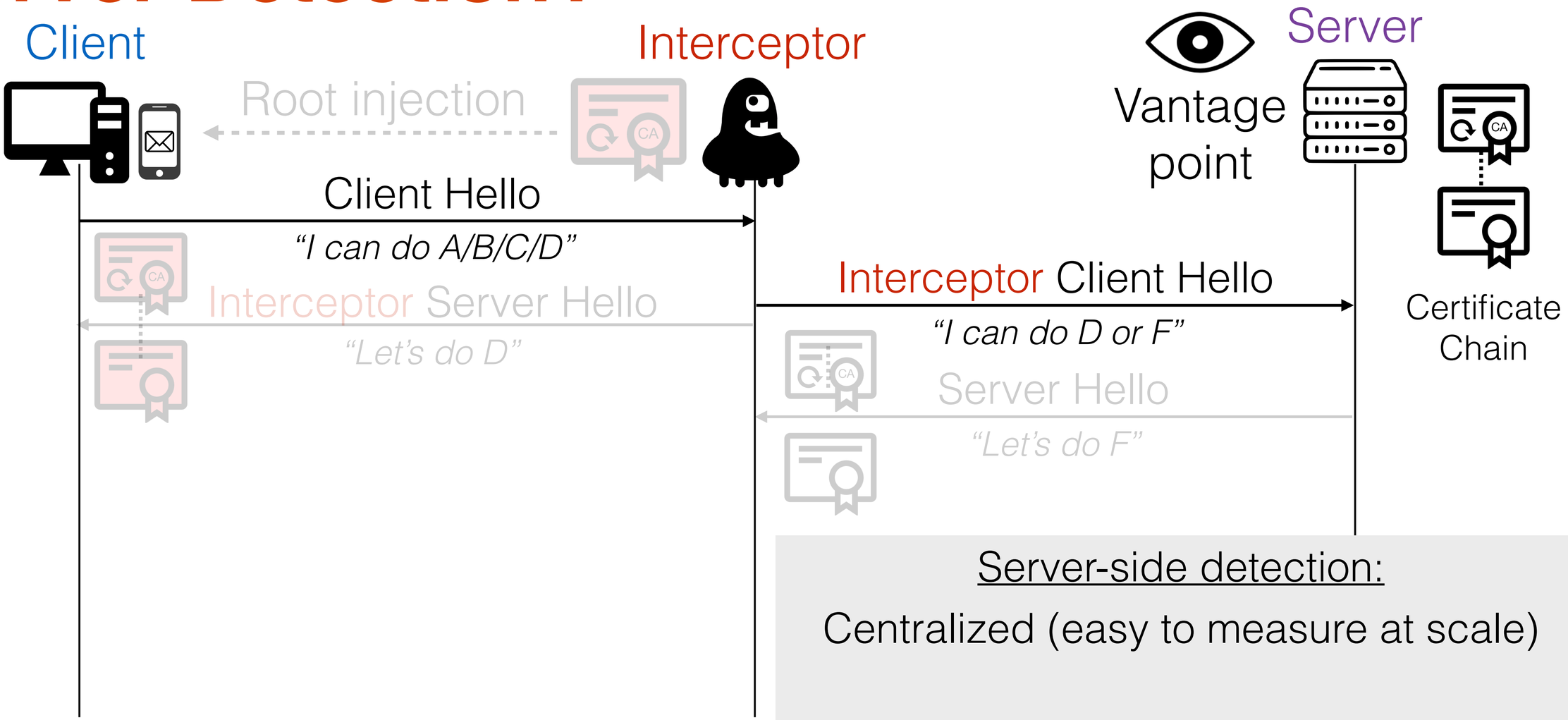
Client-side detection:

Distributed (difficult to scale)

Requires custom instrumentation

0.2% of 3M TLS conn. intercepted

Server Detection?

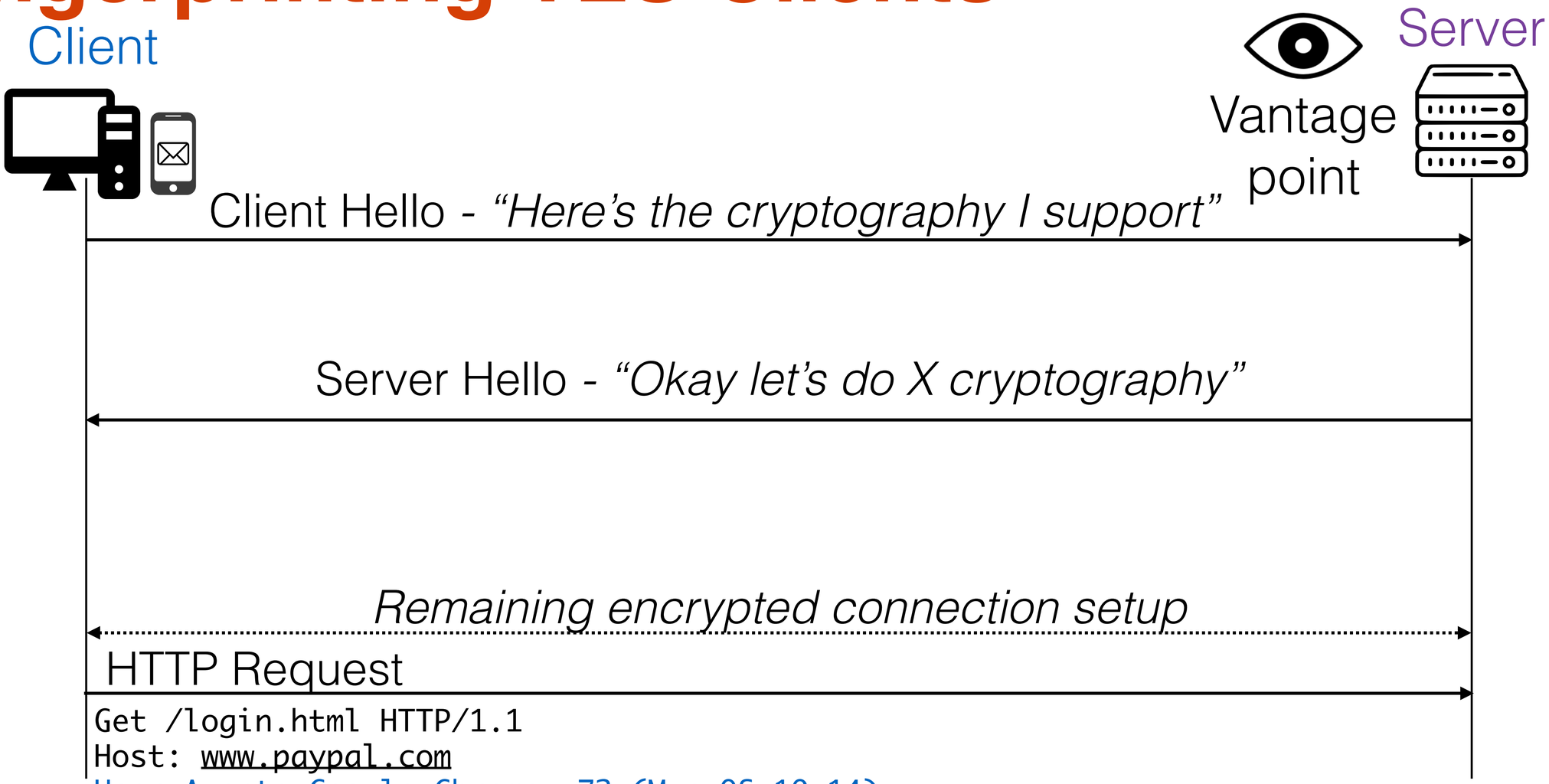


<u>Server-side detection:</u>

Centralized (easy to measure at scale)

How to know what Client Hello to expect?

Fingerprinting TLS Clients



Fingerprinting TLS Clients

Client

Server

Vantage point

Client Hello - *"Here's the cryptography I support"*

```
Version: TLS 1.2 (0x0303)
Cipher Suites
 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Extension: ec_point_formats
 EC point format: uncompressed
Extension: elliptic_curves
 secp256r1 (0x0017)
 secp256r1 (0x0018)
Extension: Application Layer Protocol Negotiation
```

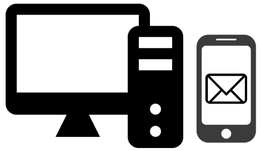
Remaining encrypted connection setup

HTTP Request

```
Get /login.html HTTP/1.1
Host: www.paypal.com
User-Agent: Google Chrome v72 (Mac OS 10.14)
```

Fingerprinting TLS Clients

Client



Client Hello

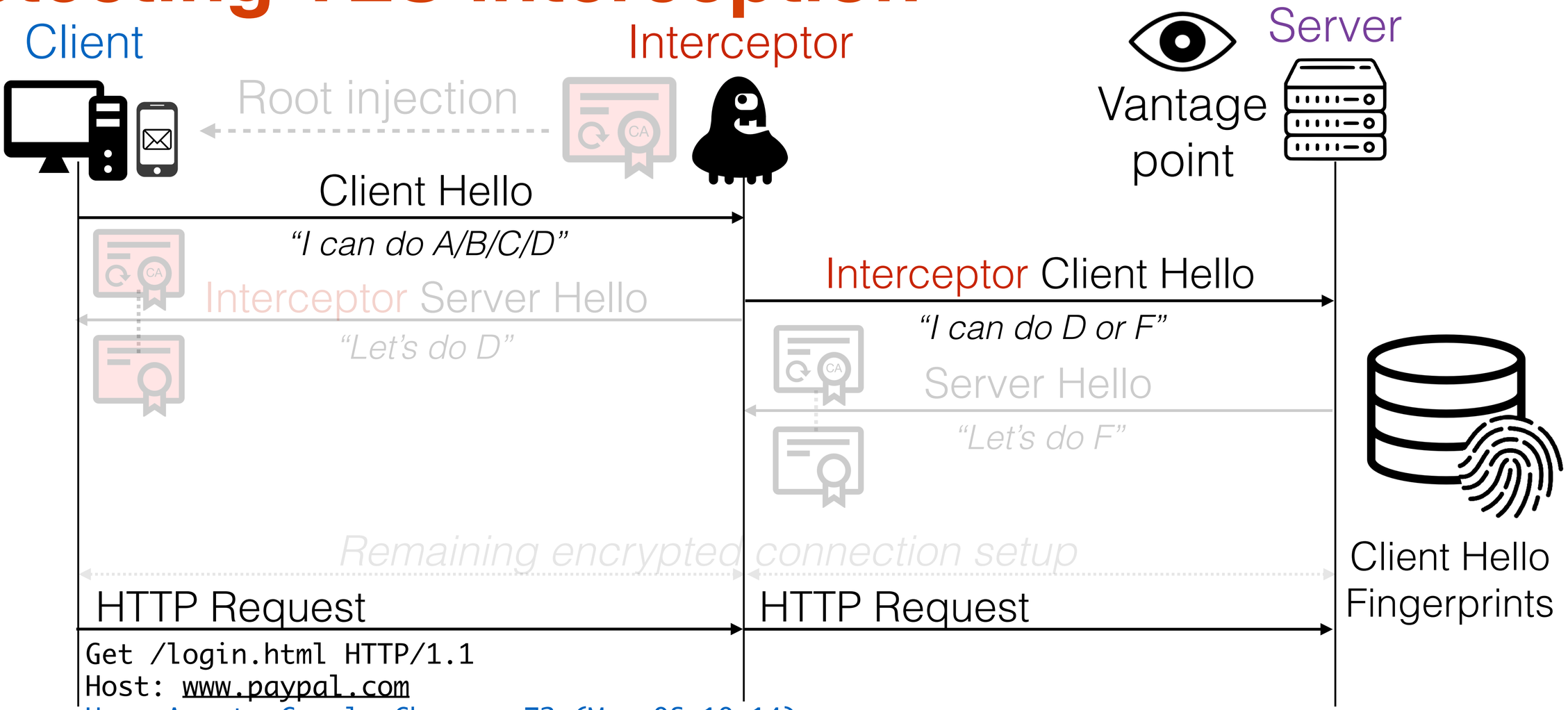
```
Version: TLS 1.2 (0x0303)
Cipher Suites
 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Extension: ec_point_formats
 EC point format: uncompressed
Extension: elliptic_curves
 secp256r1 (0x0017)
 secp256r1 (0x0018)
Extension: Application Layer Protocol Negotiation
```

HTTP Request

```
Get /login.html HTTP/1.1
Host: www.paypal.com
User-Agent: Google Chrome v72 (Mac OS 10.14)
```

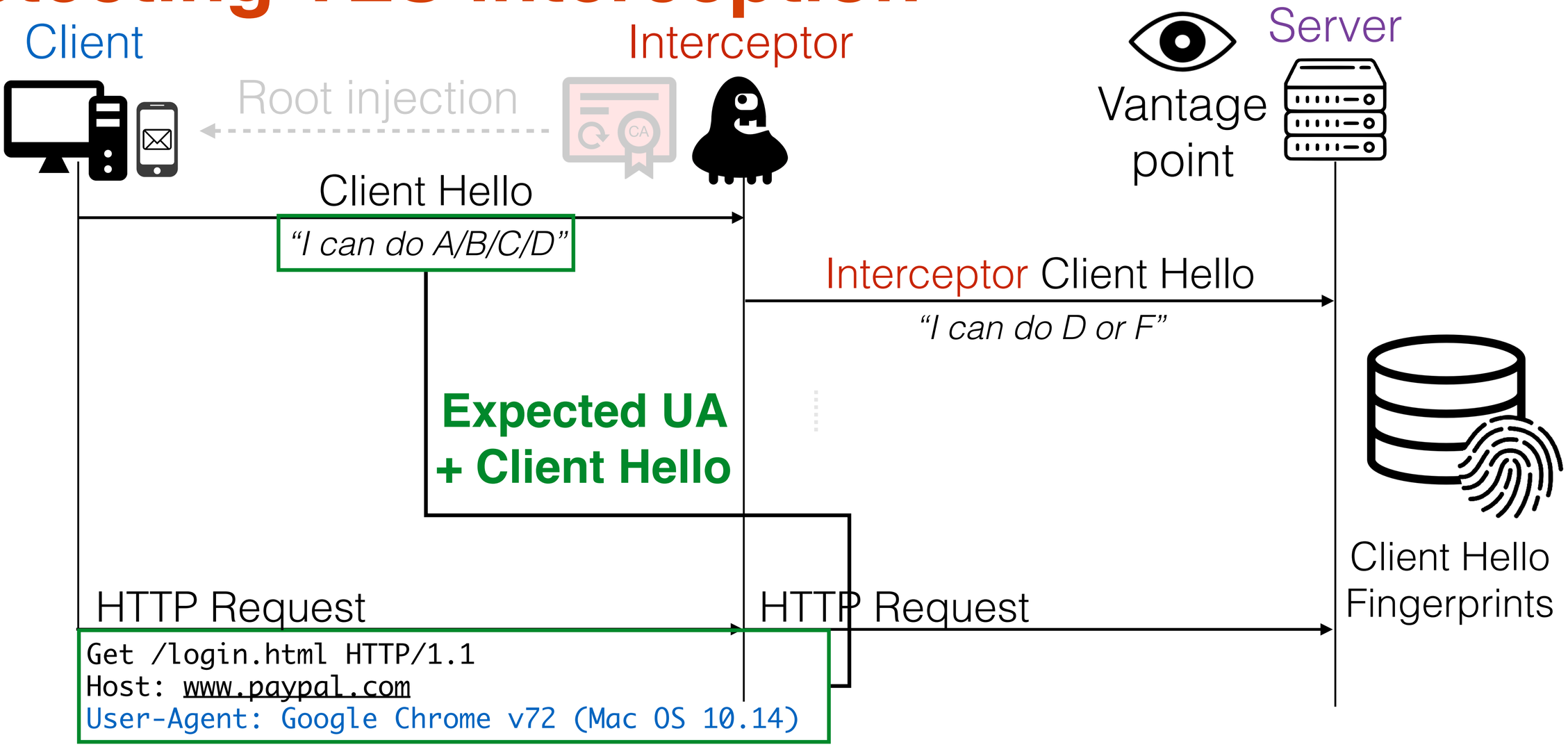
Catalog of Client Hello fingerprints for popular TLS client User-Agents (e.g., web browsers)

Detecting TLS interception

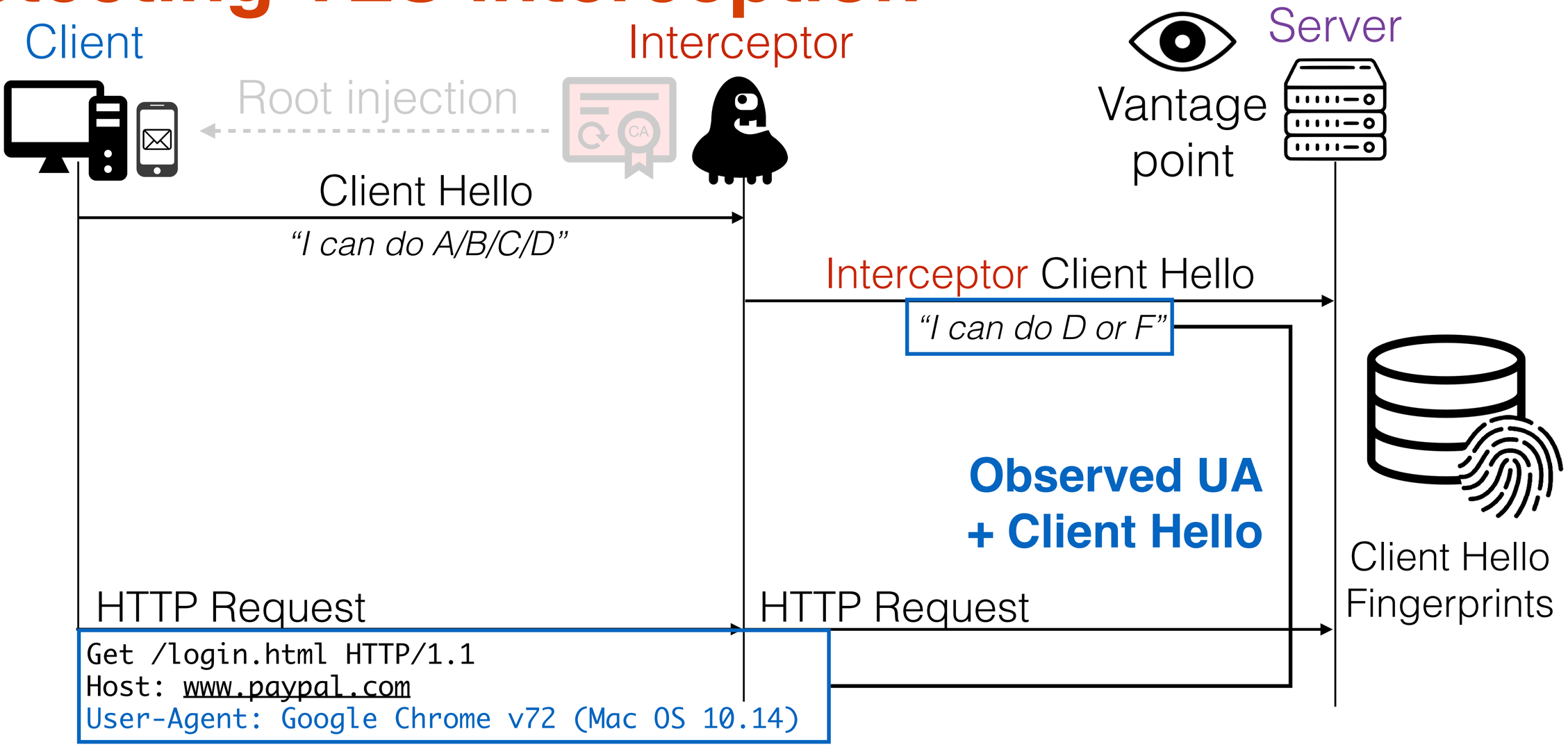



```
Get /login.html HTTP/1.1
Host: www.paypal.com
User-Agent: Google Chrome v72 (Mac OS 10.14)
```

Detecting TLS interception



Detecting TLS interception



TLS Interception Rates

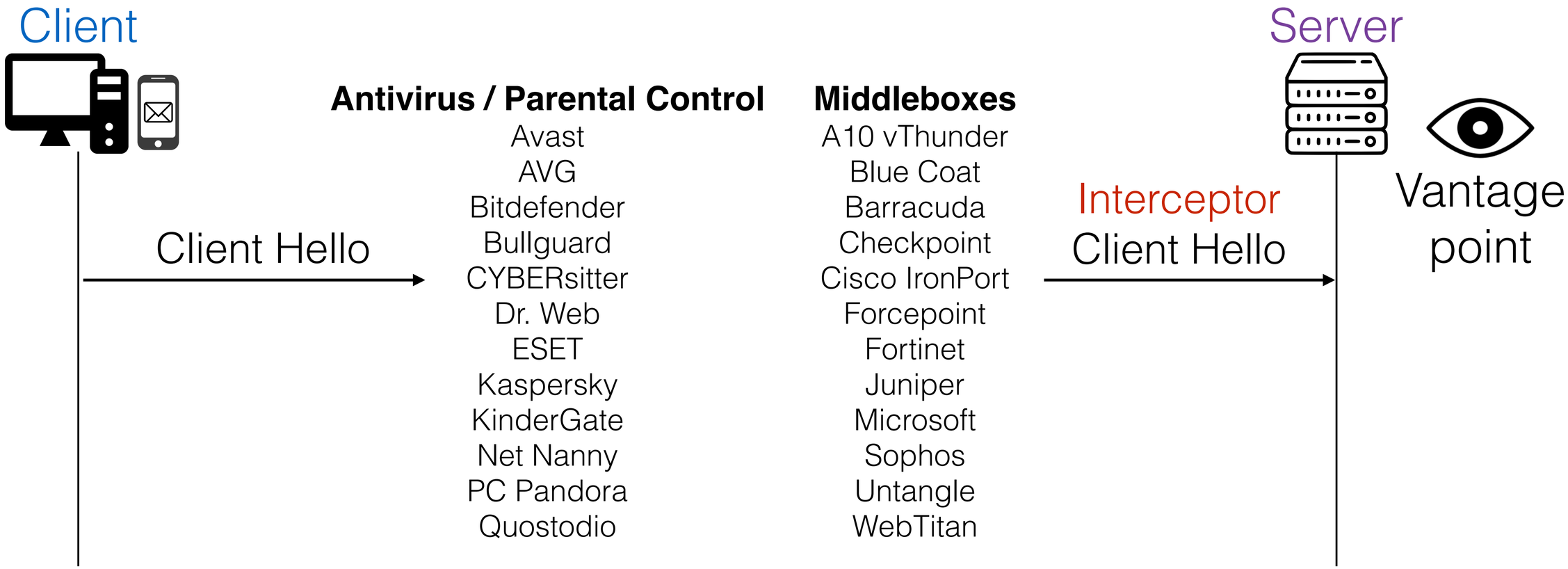
Dataset	Description
Firefox	Daily update check
Amazon	Invisible pixel load via JavaScript
Cloudflare	5% sample of all CDN traffic

2500x prior research

TLS Interception Rates

Dataset	Description	% of TLS conn. intercepted
Firefox	Daily update check	4.0%
Amazon	Invisible pixel load via JavaScript	6.2%
Cloudflare	5% sample of all CDN traffic	10.9%
	8 billion total TLS connections 2500x prior research	**20-50x more interception**

Attributing Interception



Top TLS Interceptors

Dataset	Fingerprint	% Total Interception
Firefox	*Unknown A*	17.1%
	Avast Antivirus	10.8%
	Unknown B	9.4%
	Blue Coat Middlebox	9.1%
	Unknown C	8.3%
Amazon	Avast Antivirus	9.1%
	AVG Antivirus	7.0%
	Unknown D	6.5%
	Kaspersky Antivirus	5.0%
	BitDefender Antivirus	3.1%
Cloudflare	Bouncy Castle (Android 5)	26.3%
	Bouncy Castle (Android 4)	21.6%
	Unknown E	5.0%
	ESET Antivirus	2.8%
	Dr. Web Antivirus	2.6%

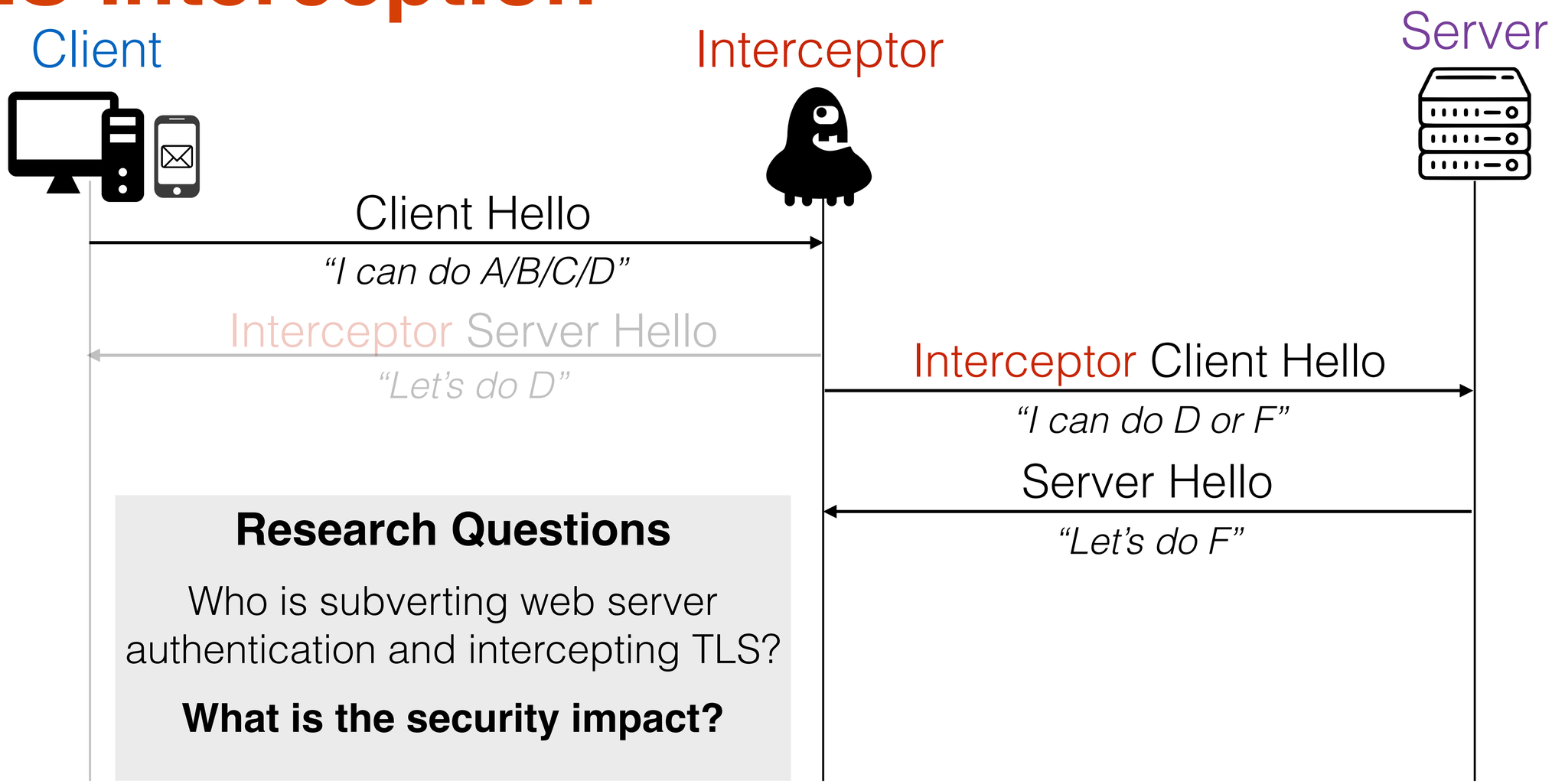
Top TLS Interceptors

Dataset	Fingerprint	% Total Interception
Firefox	*Unknown A*	17.1%
	Avast Antivirus	10.8%
	Unknown B	9.4%
	Blue Coat Middlebox	9.1%
	Unknown C	8.3%
Amazon	Avast Antivirus	9.1%
	AVG Antivirus	7.0%
	Unknown D	6.5%
	Kaspersky Antivirus	5.0%
	BitDefender Antivirus	3.1%
Cloudflare	Bouncy Castle (Android 5)	26.3%
	Bouncy Castle (Android 4)	21.6%
	Unknown E	5.0%
	ESET Antivirus	2.8%
	Dr. Web Antivirus	2.6%

Top TLS Interceptors

Dataset	Fingerprint	% Total Interception
Firefox	*Unknown A*	17.1%
	Avast Antivirus	10.8%
	Unknown B	9.4%
	Blue Coat Middlebox	9.1%
	Unknown C	8.3%
Amazon	Avast Antivirus	9.1%
	AVG Antivirus	7.0%
	Unknown D	6.5%
	Kaspersky Antivirus	5.0%
	BitDefender Antivirus	3.1%
Cloudflare	Bouncy Castle (Android 5)	26.3%
	Bouncy Castle (Android 4)	21.6%
	Unknown E	5.0%
	ESET Antivirus	2.8%
	Dr. Web Antivirus	2.6%

TLS Interception

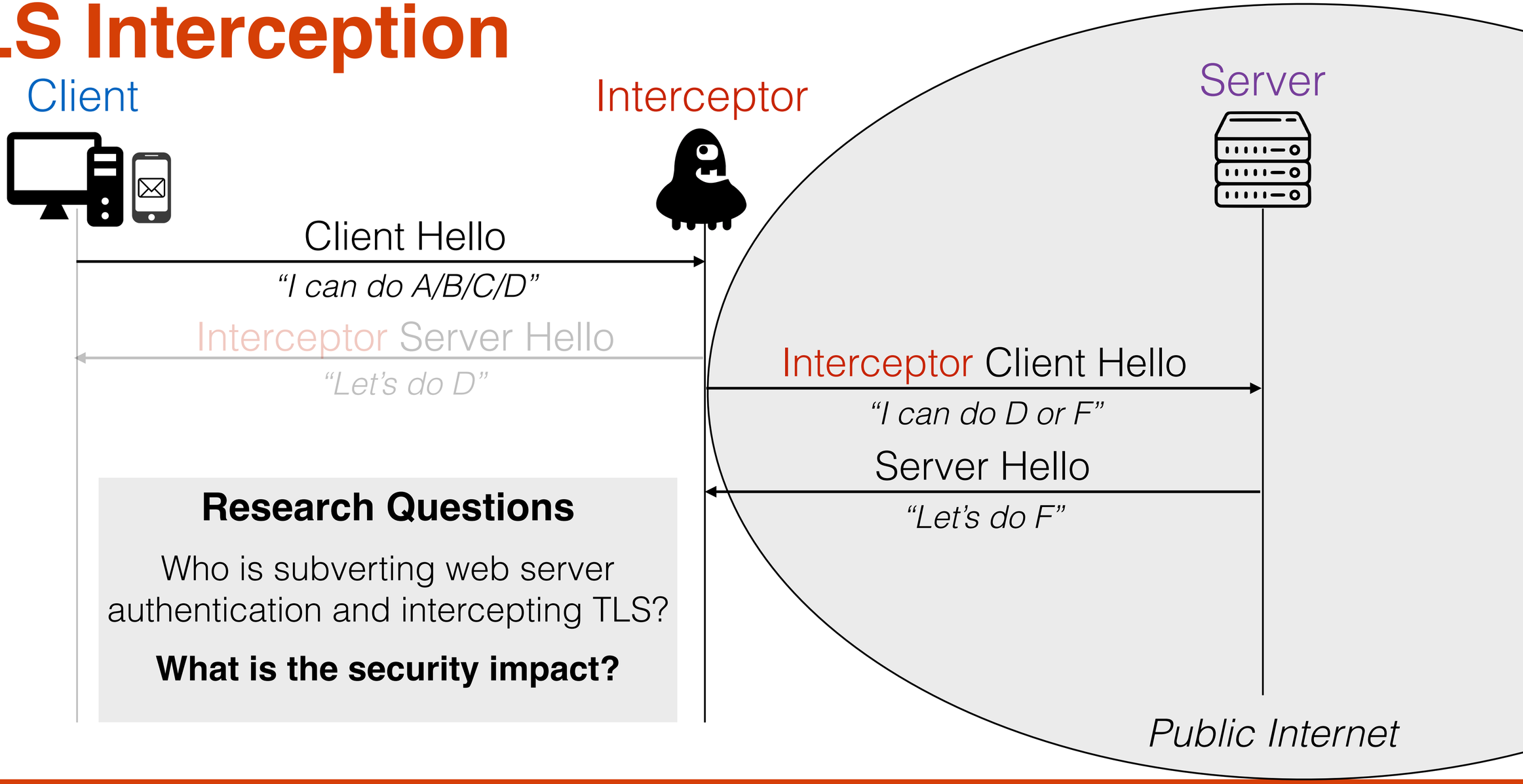


Research Questions

Who is subverting web server authentication and intercepting TLS?

What is the security impact?

TLS Interception

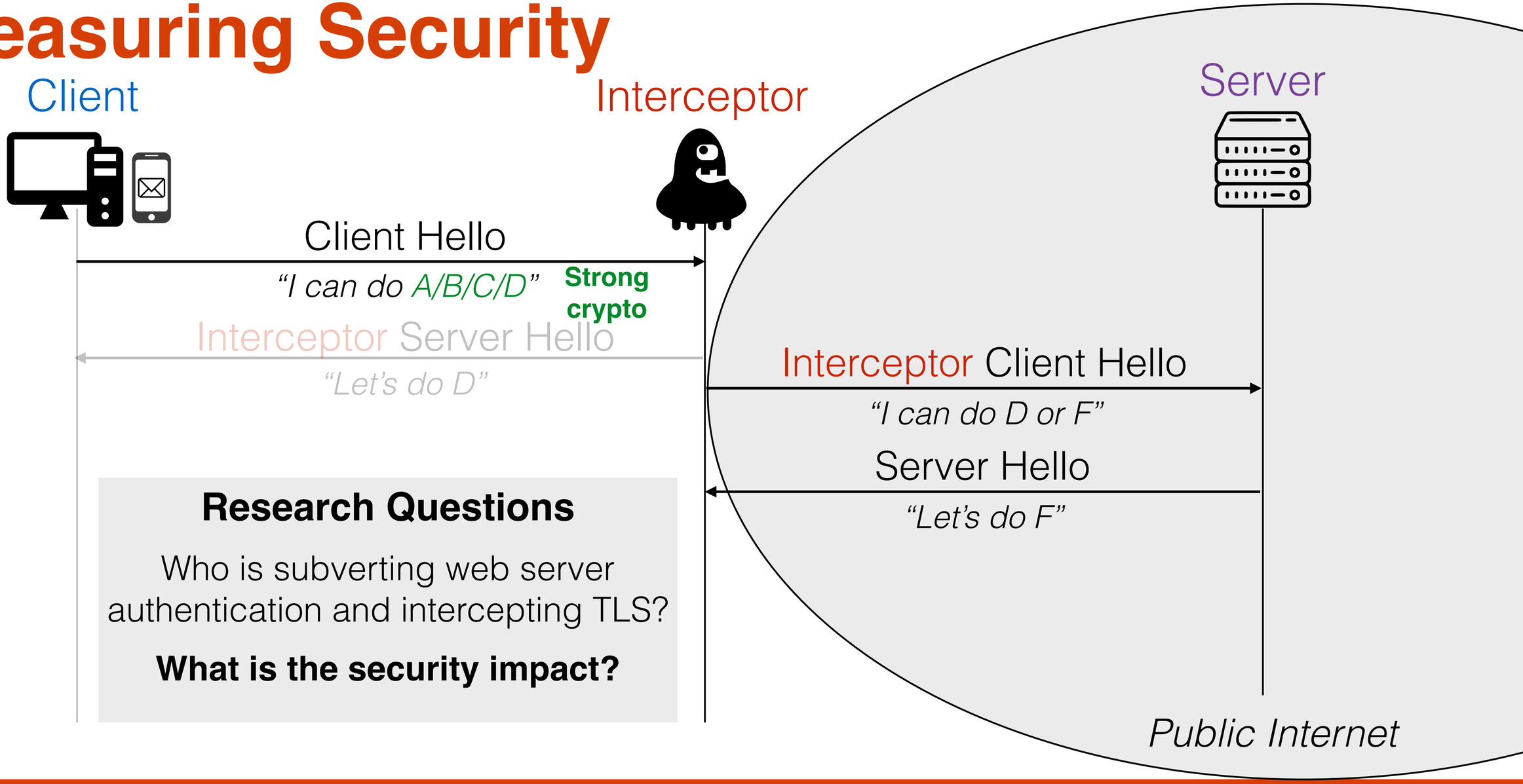


Research Questions

Who is subverting web server authentication and intercepting TLS?

What is the security impact?

Measuring Security

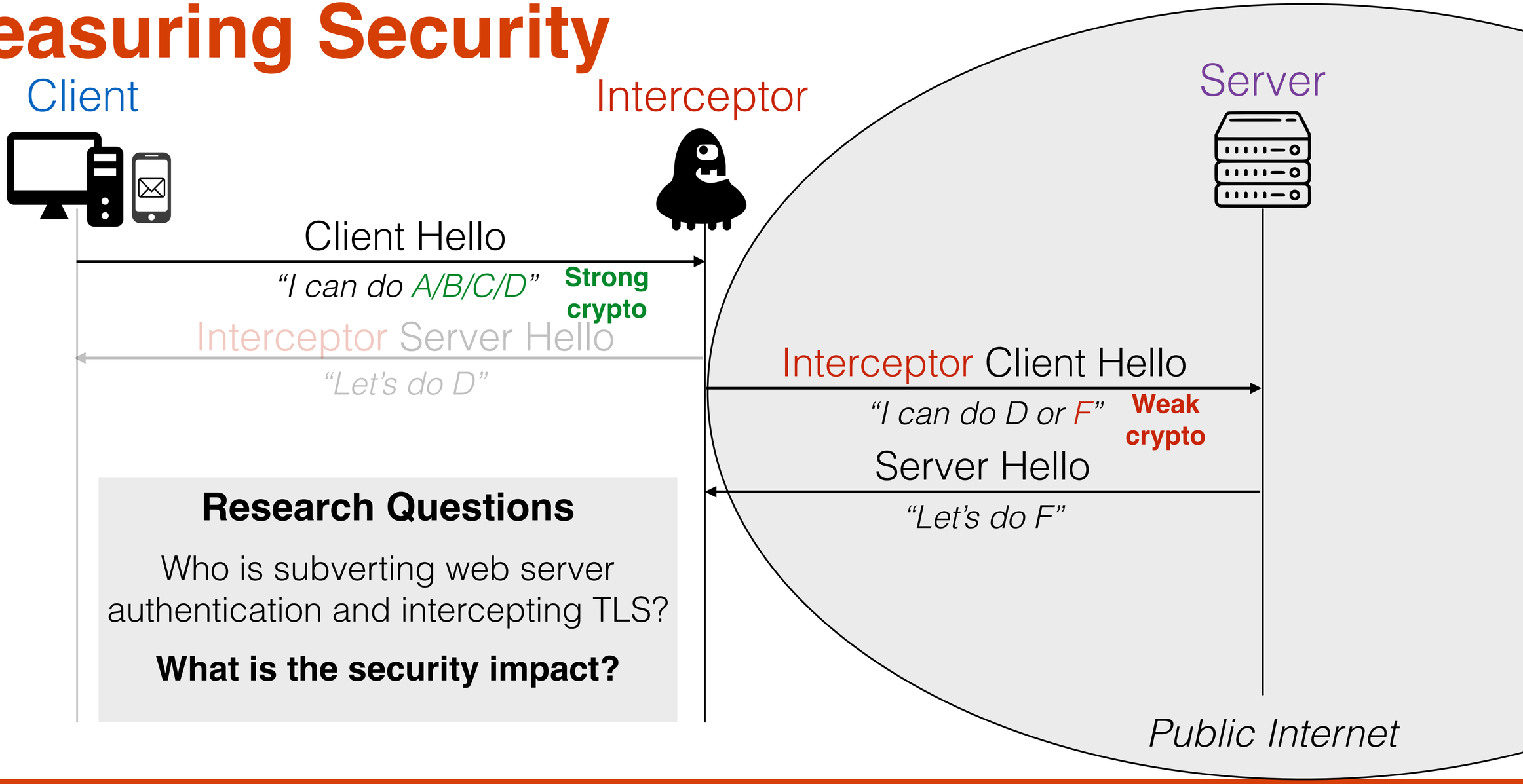


Research Questions

Who is subverting web server authentication and intercepting TLS?

What is the security impact?

Measuring Security

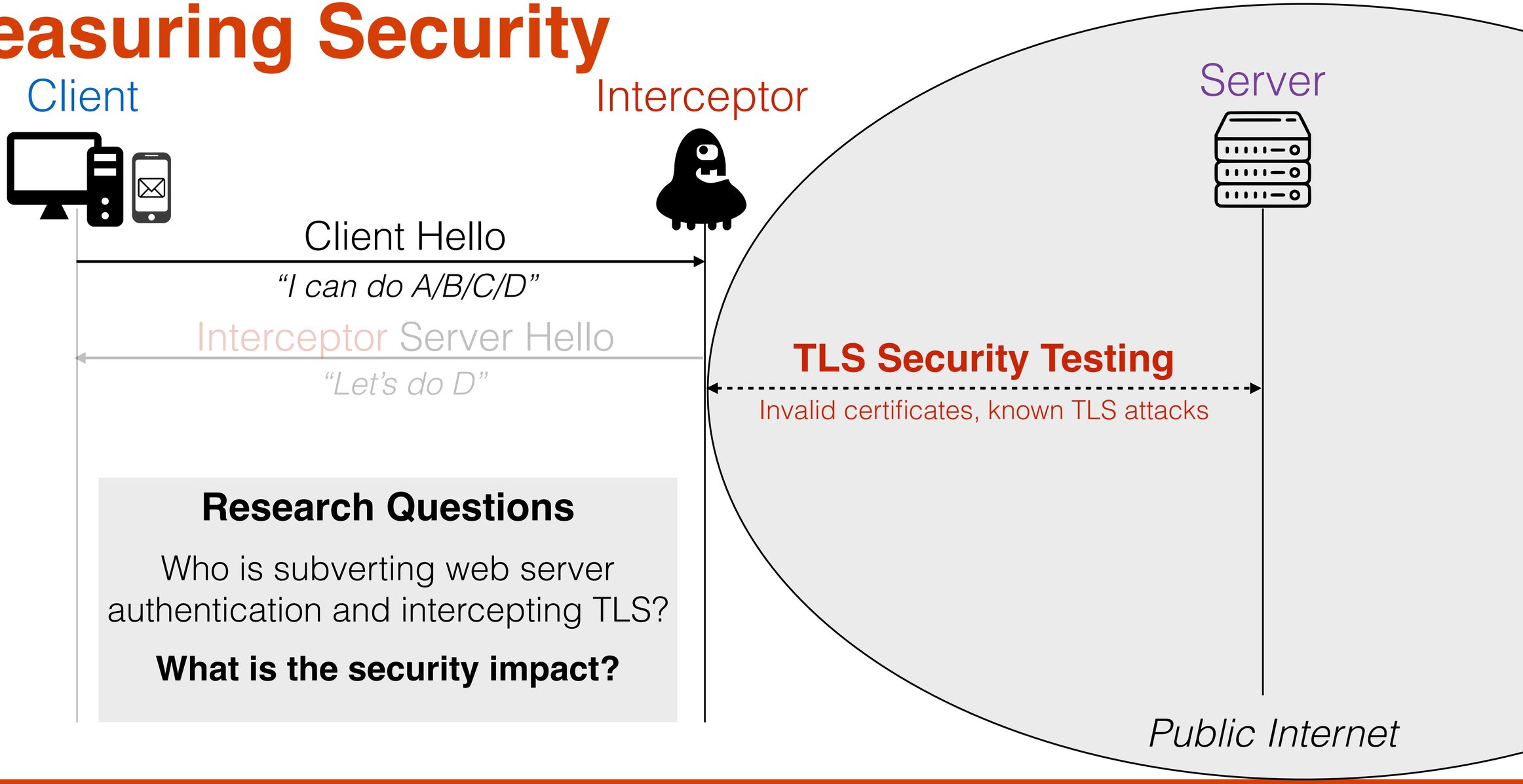


Research Questions

Who is subverting web server authentication and intercepting TLS?

What is the security impact?

Measuring Security



Research Questions

Who is subverting web server authentication and intercepting TLS?

What is the security impact?

Results

Dataset	Original Security	Intercepted Security			
		A	B	C	F
Firefox	A	34.3%	16.8%	12.2%	36.8%
Amazon	A	57.1%	2.9%	5.6%	8.1%
	B	2.7%	10.2%	1.2%	8.3%
	C	0.6%	0.4%	1.0%	0.3%
	F	0.0%	0.2%	0.1%	1.0%
Cloudflare	A	7.4%	1.1%	29.7%	10.0%
	B	0.0%	0.0%	0.0%	0.0%
	C	9.4%	3.3%	22.0%	4.5%
	F	0.8%	0.1%	0.4%	1.5%

Rubric

A = Optimal

B = Not vulnerable

C = Known attack

F = Severely broken

Results

Dataset	Original Security	Intercepted Security			
		A	B	C	F
Firefox	A	34.3%	16.8%	12.2%	36.8%
Amazon	A	57.1%	2.9%	5.6%	8.1%
	B	2.7%	10.2%	1.2%	8.3%
	C	0.6%	0.4%	1.0%	0.3%
	F	0.0%	0.2%	0.1%	1.0%
Cloudflare	A	7.4%	1.1%	29.7%	10.0%
	B	0.0%	0.0%	0.0%	0.0%
	C	9.4%	3.3%	22.0%	4.5%
	F	0.8%	0.1%	0.4%	1.5%

Rubric

A = Optimal

B = Not vulnerable

C = Known attack

F = Severely broken

Results

Dataset	Original Security	Intercepted Security			
		A	B	C	F
Firefox	A	34.3%	16.8%	12.2%	36.8%
Amazon	A	57.1%	2.9%	5.6%	8.1%
	B	2.7%	10.2%	1.2%	8.3%
	C	0.6%	0.4%	1.0%	0.3%
	F	0.0%	0.2%	0.1%	1.0%
Cloudflare	A	7.4%	1.1%	29.7%	10.0%
	B	0.0%	0.0%	0.0%	0.0%
	C	9.4%	3.3%	22.0%	4.5%
	F	0.8%	0.1%	0.4%	1.5%

Rubric

A = Optimal

B = Not vulnerable

C = Known attack

F = Severely broken

Results

Dataset	Original Security	Intercepted Security			
		A	B	C	F
Amazon (all traffic)	A	57.1%	2.9%	5.6%	8.1%
	B	2.7%	10.2%	1.2%	8.3%
	C	0.6%	0.4%	1.0%	0.3%
	F	0.0%	0.2%	0.1%	1.0%
Amazon (middlebox)	A	13.5%	3.0%	0.8%	18.0%
	B	0.7%	23.3%	0.6%	37.8%
	C	0.1%	0.1%	0.0%	2.2%
	F	0.0%	0.0%	0.0%	0.0%

Rubric

A = Optimal

B = Not vulnerable

C = Known attack

F = Severely broken

Interceptor Transparency

US Computer Emergency Readiness Team (US-CERT) issued alert [1]

6 vendors patched vulnerabilities

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alert (TA17-075A)

HTTPS Interception Weakens TLS Security

Original release date: March 16, 2017

Print Tweet Send Share

Systems Affected

All systems behind a hypertext transfer protocol secure (HTTPS) interception product are potentially affected.

[1] https://www.cisa.gov/uscert/ncas/alerts/TA17-075A

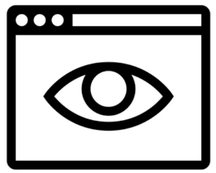
Interceptor Transparency

US Computer Emergency Readiness Team (US-CERT) issued alert [1]

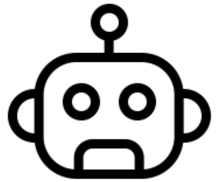
6 vendors patched vulnerabilities

Prompted Cloudflare to deploy continuous, automated monitoring [2]

ClientHello fingerprints popularized by Salesforce as JA3; used to detect:



Censorship detection



Bot detection

IoT detection

[1] https://www.cisa.gov/uscert/ncas/alerts/TA17-075A

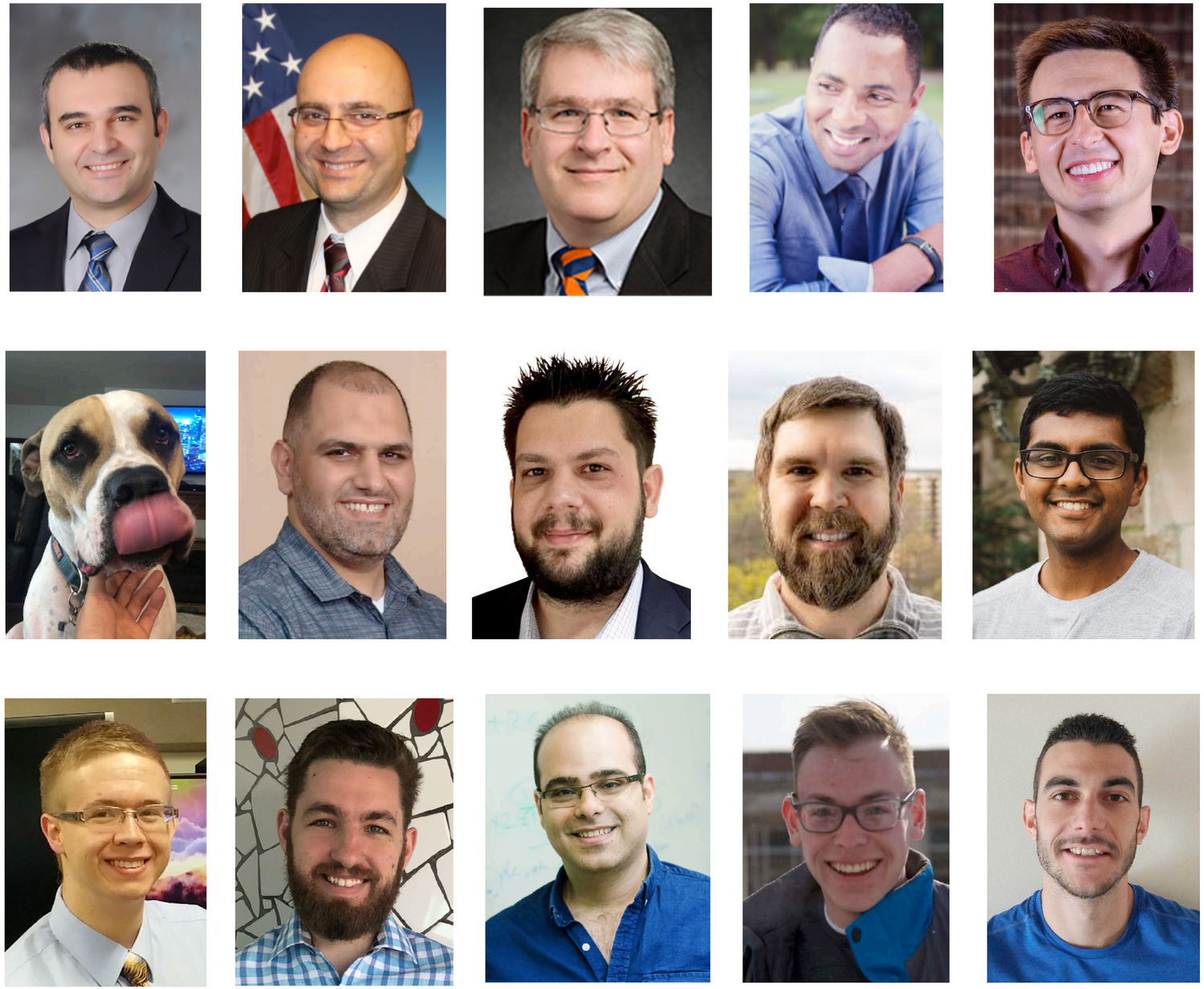
[2] https://malcolm.cloudflare.com/

Collaborators

Georgia Tech

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

Stanford University



Peeking into the Web PKI

Uncovering the Trust That Sustains Web Server Authentication

Zane Ma (he/him)
Oregon State University
2024.05.02

Stale TLS Certificates

Investigating Precarious Third-Party Access to Valid TLS Keys

Zane Ma (he/him)
Oregon State University
2023.10.25

Aaron Faulkenberry, Thomas Papastergiou, Zakir Durumeric*, Michael Bailey, Angelos Keromytis, Fabian Monrose, Manos Antonakakis

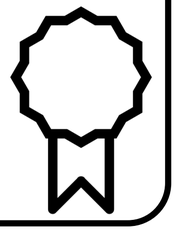
Georgia Institute of Technology *Stanford University

Public-key crypto

Issuer Name: Certificate Authority XYZ

Subject Name: domain.com
Subject Public Key: 0400aefa6edef14a…

Issuer Signature: 19574503953e…



TLS Certificate

Key challenge: linking cryptographic identity (public-key) with semantic identity

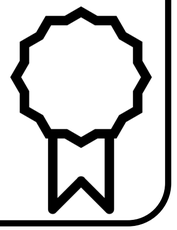
TLS certificate = cached attestation

Issuer Name: Certificate Authority XYZ

Subject Name: domain.com
Subject Public Key: 0400aefa6edef14a…

Validity: 2023-10-20 to 2024-11-19

Issuer Signature: 19574503953e…



TLS Certificate

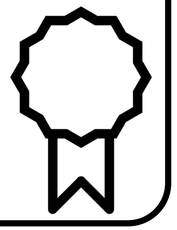
TLS certificate = cached attestation

Issuer Name: Certificate Authority XYZ

Subject Name: domain.com
Subject Public Key: 0400aefa6edef14a…

Validity: 2023-10-20 to 2024-11-19

Issuer Signature: 19574503953e…



TLS Certificate

Stale TLS certificates

Issuer Name: Certificate Authority XYZ

Subject Name: domain.com
Subject Public Key: 0400aefa6edef14a…

Validity: 2023-10-20 to 2024-11-19

Issuer Signature: 19574503953e…

Stale TLS Certificate

Issuer Name: Certificate Authority XYZ

Subject Name: domain.com
Subject Public Key: 00c946d6e746f1…

Validity: 2023-10-25 to 2024-11-24

Issuer Signature: 19574503953e…

New TLS Certificate

Stale certificates arise from **certificate invalidation events**: changes to attested information (e.g., subject / issuer info) while certificate is still valid

Stale TLS certificates

Issuer Name: Certificate Authority XYZ

Subject Name: domain.com
Subject Public Key: 0400aefa6edef14a…

Validity: 2023-10-20 to 2024-11-19

Issuer Signature: 19574503953e…

Stale TLS Certificate

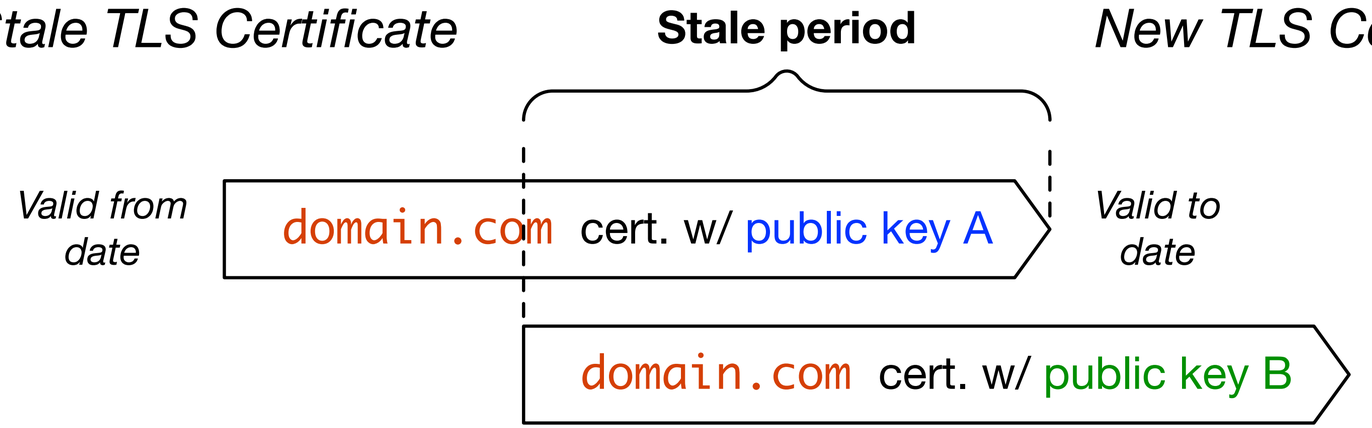
Issuer Name: Certificate Authority XYZ

Subject Name: domain.com
Subject Public Key: 00c946d6e746f1…

Validity: 2023-10-25 to 2024-11-24

Issuer Signature: 19574503953e…

New TLS Certificate



Domain-to-key operational gap

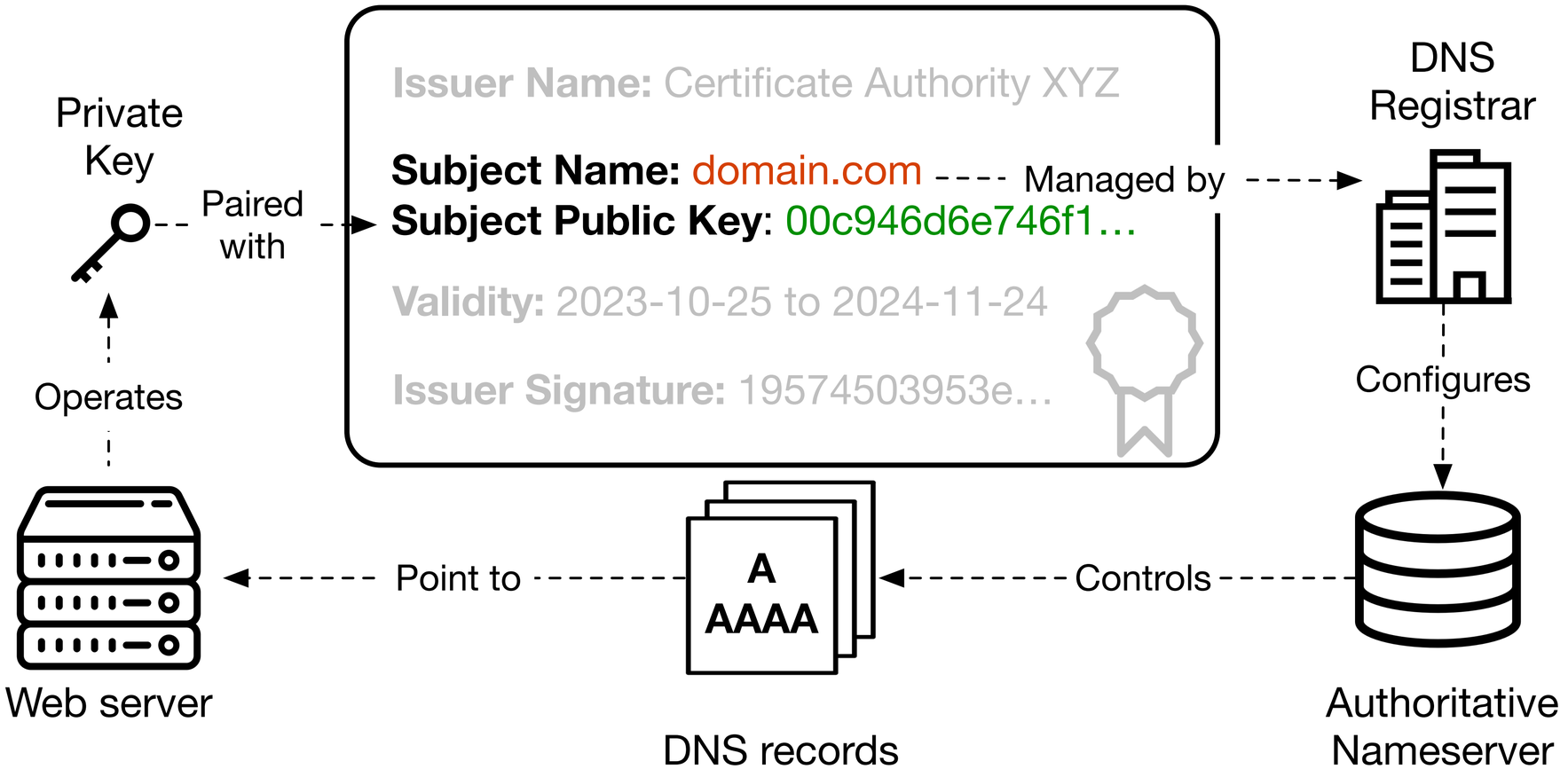
Issuer Name: Certificate Authority XYZ

Subject Name: domain.com
Subject Public Key: 00c946d6e746f1…

Validity: 2023-10-25 to 2024-11-24

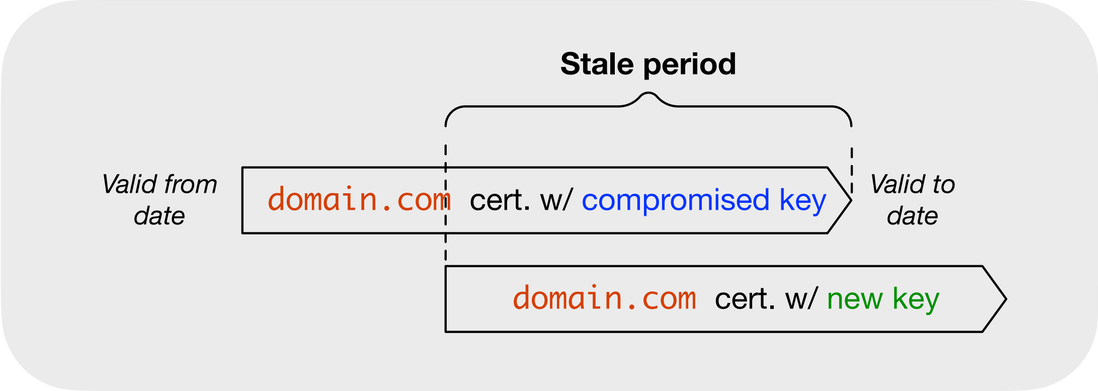
Issuer Signature: 19574503953e…

Domain-to-key operational gap



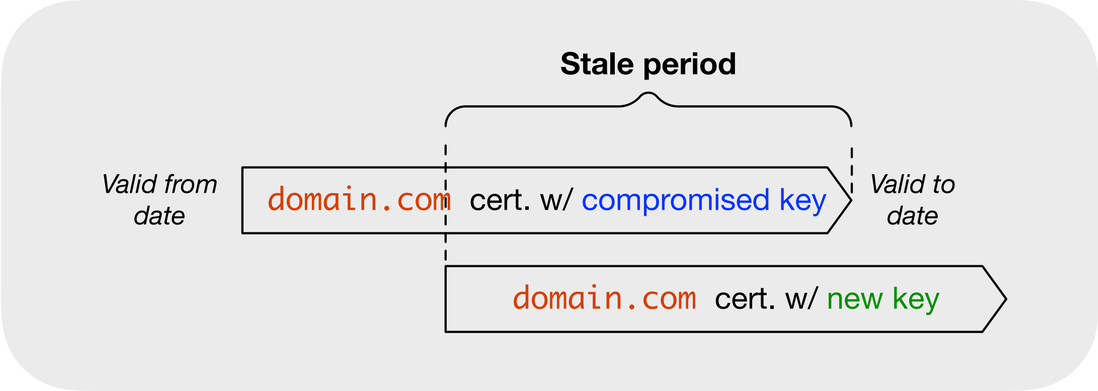
Third-party access to valid TLS keys

Compromised key change

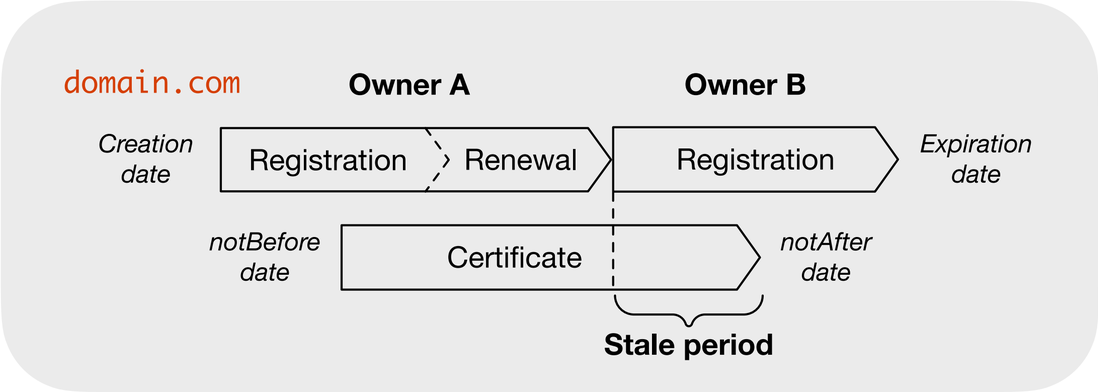


Third-party access to valid TLS keys

Compromised key change

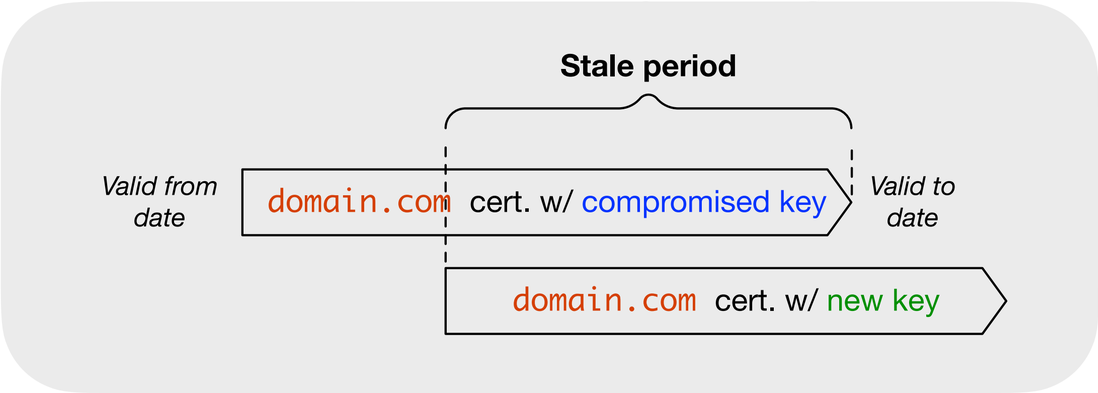


Domain owner change

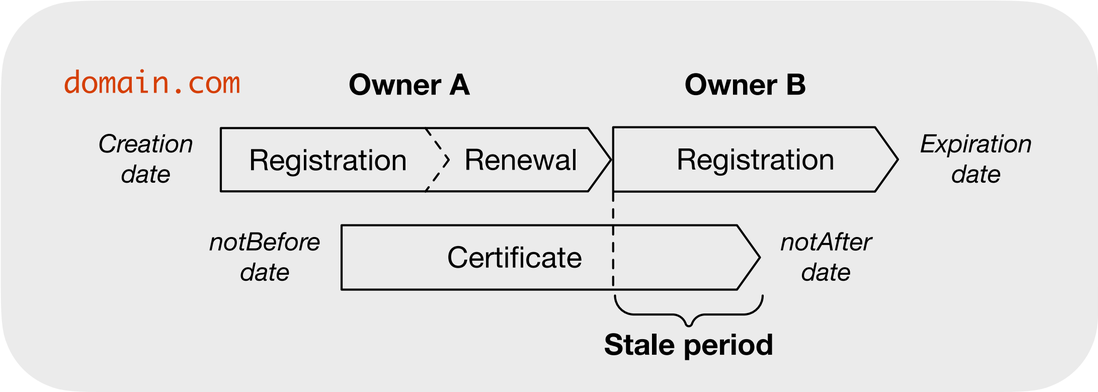


Third-party access to valid TLS keys

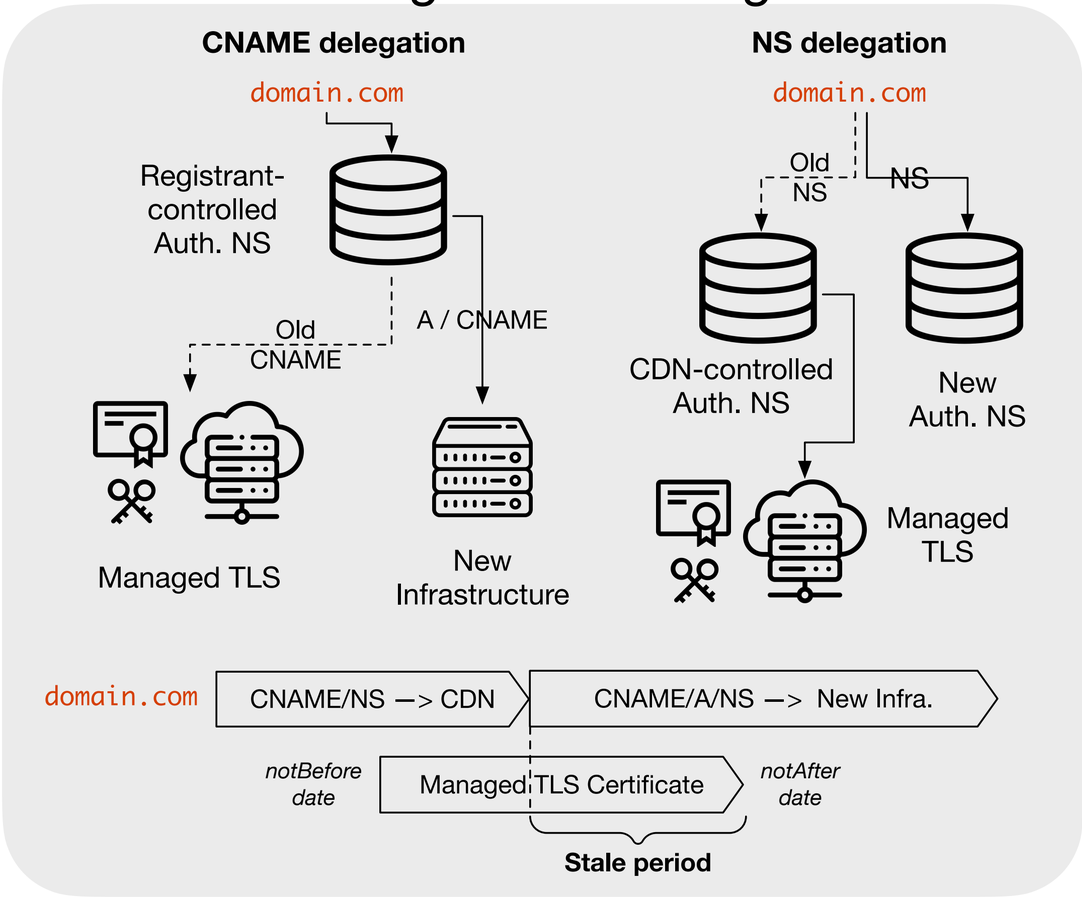
Compromised key change



Domain owner change



Managed TLS change



Revocation to the rescue?

Web browsers

Chrome has CRLsets primarily
for “emergency situations”

Firefox OCSP checking fails open
OCSP Must-Staple fails closed,
but low adoption

No revocation checking for most leaf certificate revocation

Revocation to the rescue?

Web browsers

Chrome has CRLsets primarily for “emergency situations”

Firefox OCSP checking fails open
OCSP Must-Staple fails closed, but low adoption

No revocation checking for most leaf certificate revocation

Non-browser TLS clients

openSSL, curl, API libraries, email servers, messaging clients

OpenSSL Cryptography and SSL/TLS Toolkit

curl://

OkHttp

LibreSSL

GnuTLS

Mbed TLS

BoringSSL

Minimal-to-no revocation checking

Revocation to the rescue?

Web browsers

Chrome has CRLsets primarily for “emergency situations”

Firefox OCSP checking fails open
OCSP Must-Staple fails closed, but low adoption

No revocation checking for most leaf certificate revocation

Non-browser TLS clients

openSSL, curl, API libraries, email servers, messaging clients

OpenSSL Cryptography and SSL/TLS Toolkit

curl://

OkHttp

LibreSSL

GnuTLS

Mbed TLS

BoringSSL

Minimal-to-no revocation checking

Revocation is sparse and unreliable

Internet-wide staleness

5B TLS certificates

4B WHOIS records

27B DNS records

31M Revocations

Internet-wide staleness

5B TLS certificates

4B WHOIS records

27B DNS records

31M Revocations

Third-party Staleness	# certs / day	# FQDNs / day	#e2LD / day
Key compromise	493	787	347

Internet-wide staleness

5B TLS certificates

4B WHOIS records

27B DNS records

31M Revocations

Third-party Staleness	# certs / day	# FQDNs / day	#e2LD / day
Key compromise	493	787	347
Domain owner change	2,593	2,807	1,214

Internet-wide staleness

5B TLS certificates

4B WHOIS records

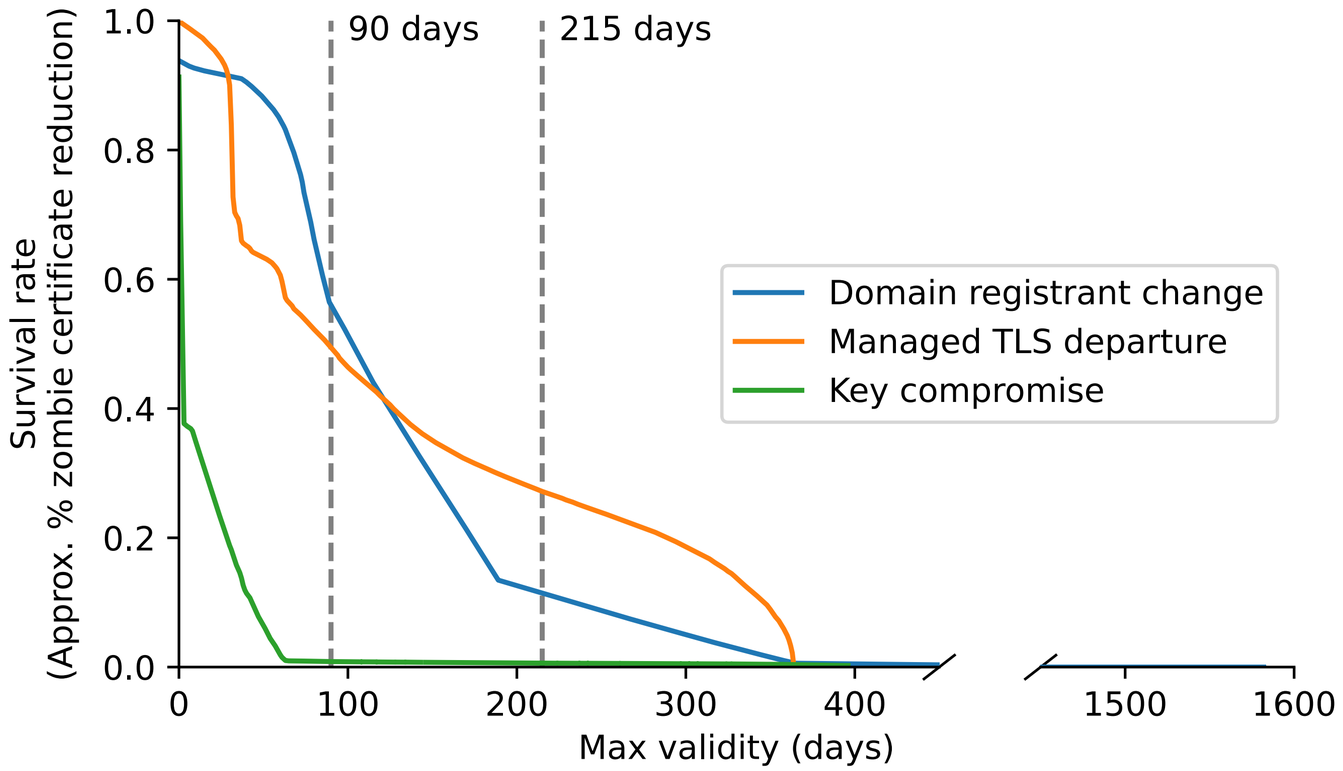
27B DNS records

31M Revocations

Third-party Staleness	# certs / day	# FQDNs / day	#e2LD / day
Key compromise	493	787	347
Domain owner change	2,593	2,807	1,214
Cloudflare managed TLS change	9,495	18,833	7,722

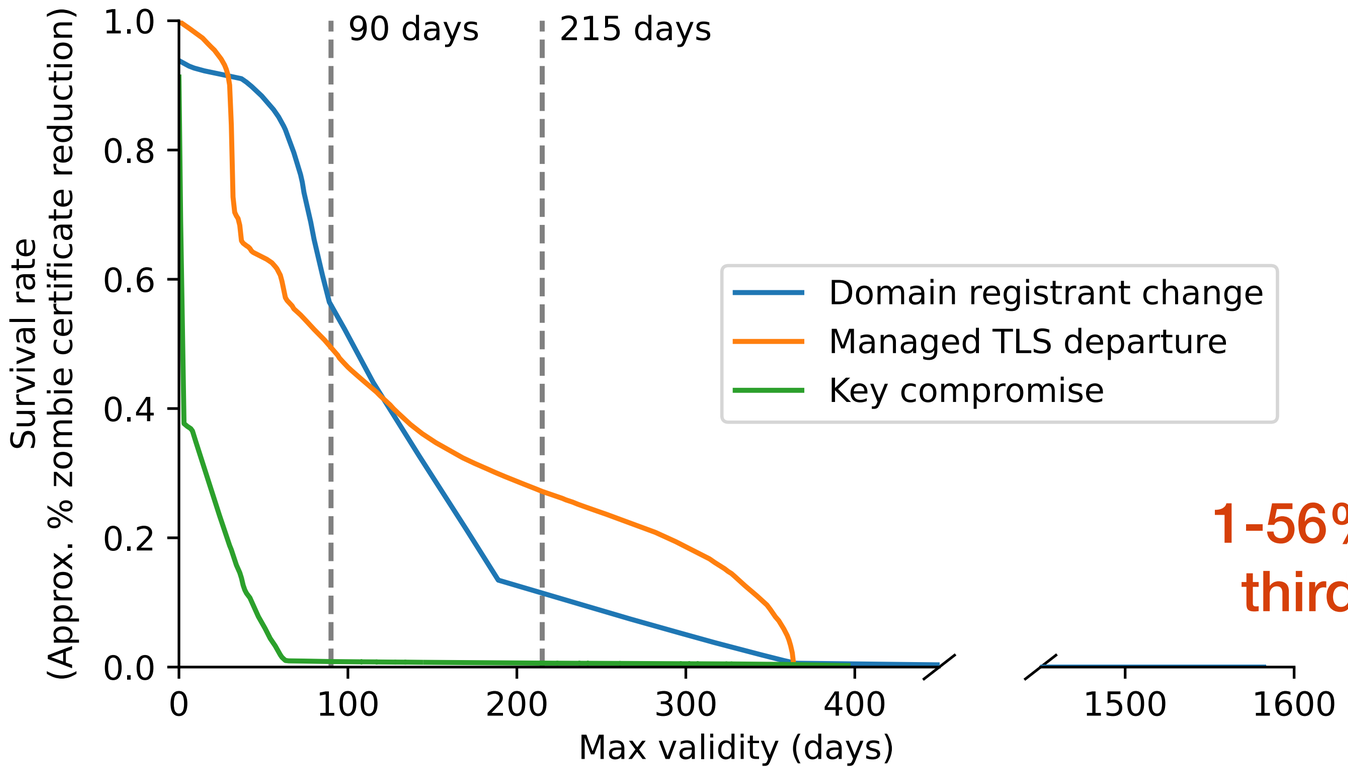
What can we do about it?

- Revocation is largely ineffective, and (unsurprisingly) poorly utilized
- Caching problem: reduce certificate lifetimes



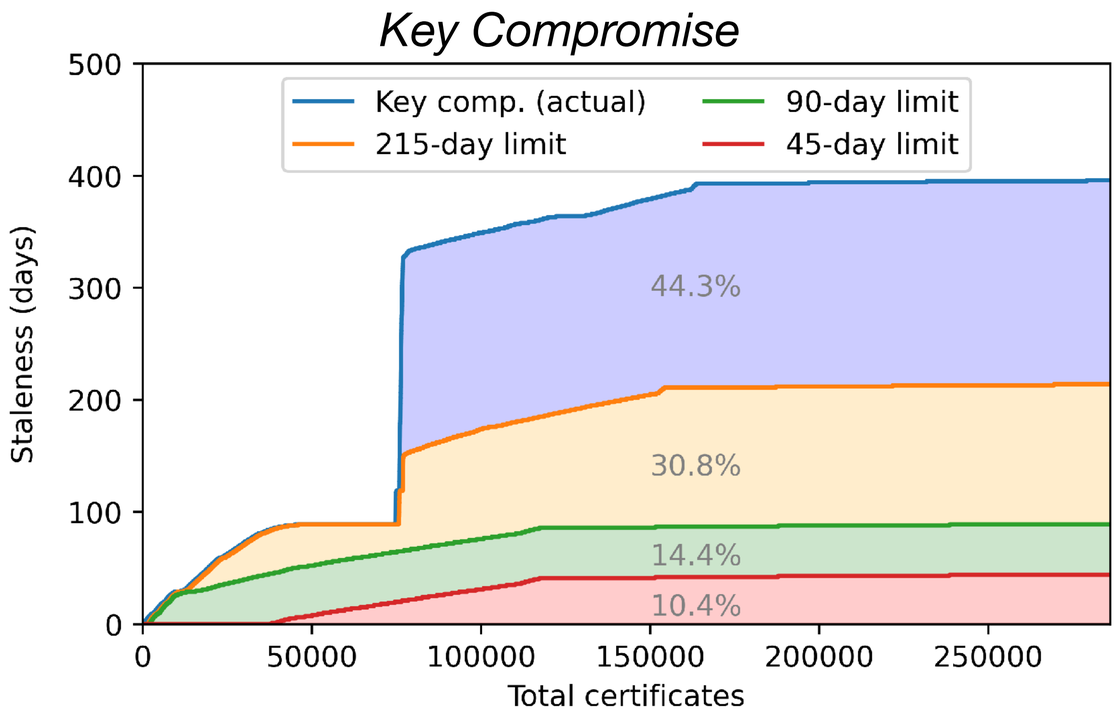
What can we do about it?

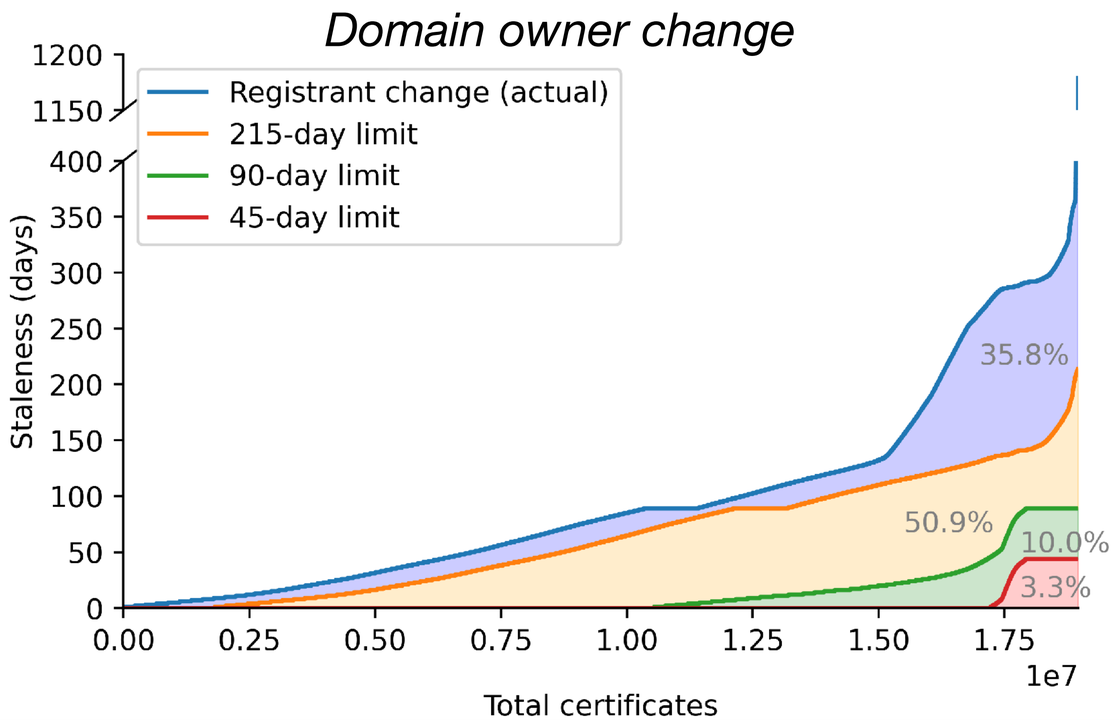
- Revocation is largely ineffective, and (unsurprisingly) poorly utilized
- Caching problem: reduce certificate lifetimes



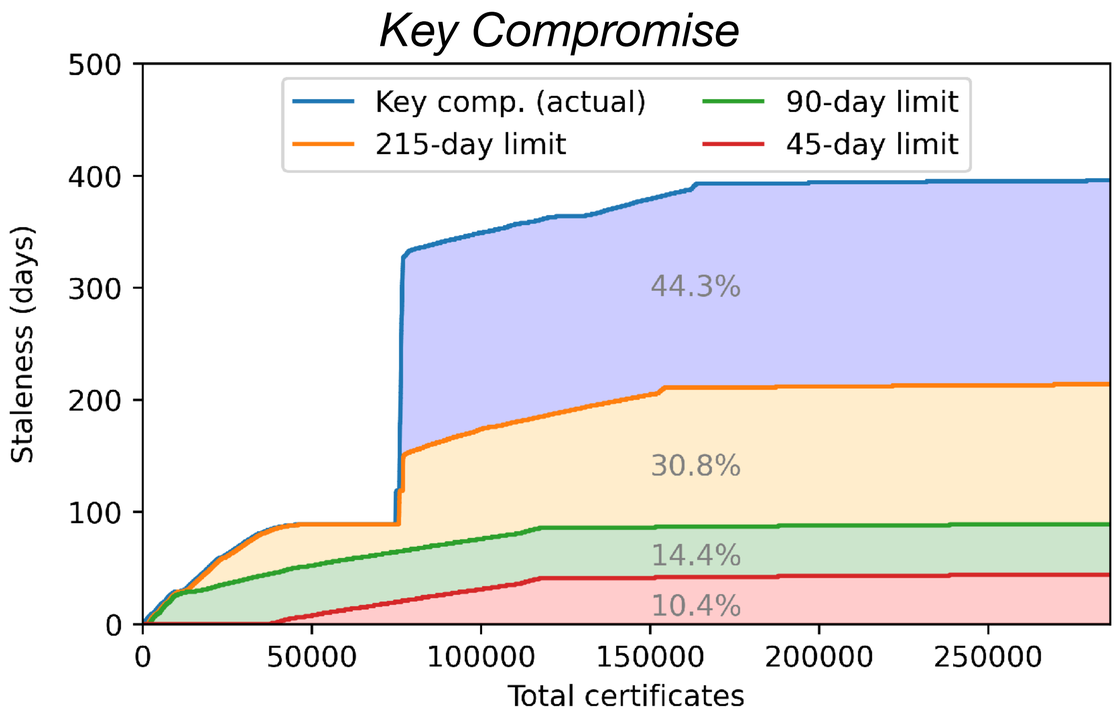
90-day limit = 1-56% reduction in stale third-party certificates

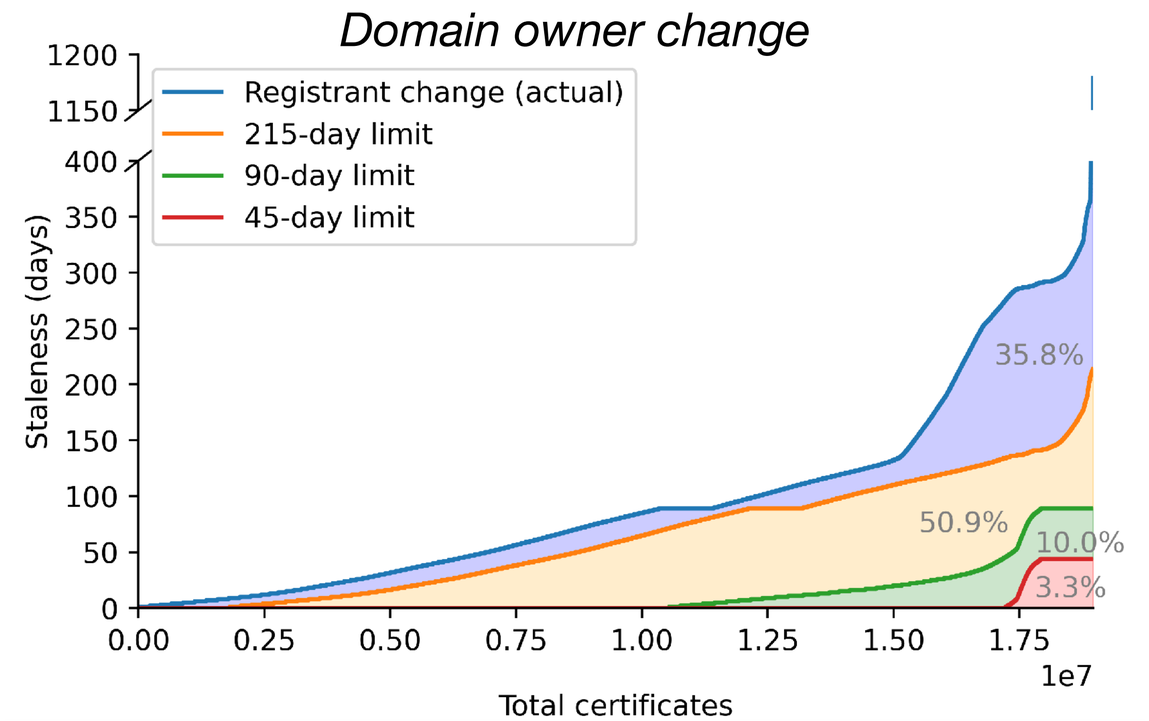
Shortening certificate lifetimes





Shortening certificate lifetimes





90-day limit =
75% decrease in time of third-party access to valid TLS keys

Conclusion

- TLS certificates are a caching mechanism to bind domain-to-key
- Stale TLS certificates —> third-party access to valid TLS keys for someone else's domain, enabling interception attacks
- This has affected at least 4 million domains since 2013

Conclusion

- TLS certificates are a caching mechanism to bind domain-to-key
- Stale TLS certificates —> third-party access to valid TLS keys for someone else's domain, enabling interception attacks
- This has affected at least 4 million domains since 2013
- Revocation (cache invalidation) is ineffective; reducing certificate lifetimes (cache duration) is a promising direction
- Alternative solutions: placing keys closer to names and reducing the domain-to-key operational gap

Stale TLS Certificates

Investigating Precarious Third-Party Access to Valid TLS Keys

Zane Ma (he/him)
Oregon State University
2023.10.25

Aaron Faulkenberry, Thomas Papastergiou, Zakir Durumeric*, Michael Bailey, Angelos Keromytis, Fabian Monrose, Manos Antonakakis

Georgia Institute of Technology *Stanford University